

**Matthew Bennett**

Foreword by:

**Tim Childe**

FLPI, CompTIA A+, Network+, Security+, MCT, MCE, MCSE  
Head of Teaching and Learning, *Netcom Training Ltd*

# CompTIA A+ Certification Guide (220-901 and 220-902)

An all-in-one study guide with full practice tests



**Packt**>

# **CompTIA A+ Certification Guide (220-901 and 220-902)**

Your IT career starts here

Matthew Bennett



**BIRMINGHAM - MUMBAI**

# CompTIA A+ Certification Guide (220-901 and 220-902)

Copyright © 2017 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing, and its dealers and distributors will be held liable for any damages caused or alleged to be caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

First published: September 2017

Production reference: 1220917

Published by Packt Publishing Ltd.  
Livery Place  
35 Livery Street  
Birmingham  
B3 2PB, UK.



ISBN 978-1-78712-730-2

[www.packtpub.com](http://www.packtpub.com)



# Credits

<b>Author</b>  Matthew Bennett	<b>Copy Editor</b>  Safis Editing
<b>Reviewers</b>  Mark Dunkerley  Tcat Houser	<b>Project Coordinator</b>  Judie Jose
<b>Commissioning Editor</b>  Kartikey Pandey	<b>Proofreader</b>  Safis Editing

<b>Acquisition Editor</b> Meeta Rajani	<b>Indexer</b> Aishwarya Gangawane
<b>Content Development Editor</b> Abhishek Jadhav	<b>Graphics</b> Kirk D'Penha
<b>Technical Editor</b> Aditya Khadye	<b>Production Coordinator</b> Aparna Bhagat



# Foreword

A lot has changed over the years. When I started in IT in the early 1990s, it was possible to get a job in IT just because you had an interest, a bit of knowledge, and a lot of enthusiasm. You could then learn as you went along, picking up a set of skills around what you were exposed to, and building up your experience.

Those days are long gone. Now you need a set of basic skills across a wide range of systems and software. Competition for jobs now is much higher, and you also need to be able prove these skills whether to get your first job in IT or to progress up the ladder of your IT career.

Although experience is always valuable, it is hard to quantify and can often have gaps in key areas if your career just hasn't exposed you to some things yet.

This is where certification comes in.

A certification from a recognized body shows that you have the skills an employer expects, it backs up any experience, and shows that where your experience may have gaps, you have the knowledge and the skills ready for when the inevitable 'new situation' comes along.

CompTIA is one of the most recognized bodies that provides certifications, and their A+ certification is the first of their Professional-level qualifications. It covers the foundational skills needed by anyone working in IT, such as hardware, software, troubleshooting, networking, security – well, just check the contents of this book to see. Gaining CompTIA A+ certification shows you have the skills required by employers, and also leads on to gaining more in depth networking and security skills with Network+ and Security+ – the three certifications that anyone wanting a successful career in IT should be looking to complete as the foundation of their knowledge and skills.

The wide range of skills covered by the A+ mean there is a lot to learn and understand before you are ready to take the exam and become certified. This can prove quite challenging to do without the right approach, and a good study guide is invaluable in making sure all those facts and figures, concepts, techniques, and so on, are clear and understood and that you are prepared in the best way you can be for the certification exam itself.

I have known Matthew for many years, often working together. He has a vast amount of experience in IT training at all levels, and with all types of learners and he has used that experience to create this no-nonsense study guide for A+ that will help you to progress your career in the no-nonsense world of IT.

**Tim Childe**

**FLPI, CompTIA A+, Network+, Security+, MCT, MCE, MCSE**

**Head of Teaching and Learning, Netcom Training Ltd**





# About the Author

**Matthew Bennett** is an award-winning trainer and author. He is also an IT consultant and has been working with Enterprise systems, notably Microsoft platforms, for 20 years. He is the author of the CompTIA Network+ Independent Study Guide, and this book is the second in his series that demonstrates real-world experience with vendor-led theory. He is based in what he describes as 'Sleepy Worcester' and enjoys relaxing by playing Fallout 4.

Matthew has worked with a large number of companies across the UK: Pearson, Global Knowledge, Leaping Man Group, Gloucester College, Bristol UWE University, and several others. He has worked as a school teacher for a challenging but rewarding Secondary School in Coventry, he has been an Exams Officer for Redditch Training Centre, and was commended by the Adult Learning Inspectorate for his work on systems planning and implementation.

Matthew is a cyber security specialist. His company, MBIT Training Ltd, is a leading national training provider focusing on Microsoft and CompTIA training across the UK for individuals and also for the corporate sector. Matthew is a former school governor with an interest in using IT systems within schools and is an advocate of Open Source Learning Management Systems such as Moodle. He supports the work of the National Cyber Skills Centre and is proud to be a Microsoft Certified Trainer and a Microsoft Partner.

Matthew's greatest achievement was the award of the Certificate of Achievement by the US 16th Special Troops Battalion through the delivery of Network+ and Security+ to the 504th Brigade Signals.

As a trainer he spend a lot of time helping people to unlearn things – bad habits or shortcuts. He believes passionately in vendor training because only setting up the software, or networking the correct way will not get you the best use out of it. He loves working with CompTIA's courses because although they are vendor-neutral, they do give you, as a trainer, the opportunity to show some of your experiences from different hardware providers and link content to real-life issues faced by IT staff all over the world. This book gives him the opportunity to reach out to hundreds, if not thousands of people wanting that first step on the career ladder. What better way than with the A+ certification?

This book has taken a few enjoyable months to write in-between training contracts. I have also traveled across the country--Wokingham, London, Cardiff, Bristol, Birmingham, and of course, Worcester.



# Acknowledgments

This book also would not have been possible had it not been for the excellent support from the team at Packt who have helped me put this together and by so doing reach out and help others get started.

I also want to thank my friends Anne Cartwright, Tim Childe, Zeshan Sattar, and Simon Richards, all of whom have been extremely supportive, but most of all a big hug to my wife, Hayley, who is my rock, also my son Sebbie, who makes a great cup of tea!



# About the Reviewers

**Mark Dunkerley** is a highly motivated and passionate technology leader. Mark was born in Newcastle Upon Tyne, England, and currently resides in Orlando, Florida. He holds a Bachelor of Science in Business Administration and a Master of Business Administration.

He has worked in the technology field for over 15 years and has experience in multiple technical areas. Certifications have been earned from AirWatch, Microsoft, CompTIA, VMware, AXELOS, Cisco and EMC.

Mark has been invited to speak at multiple conferences, including Microsoft and VMware events, is a published author (Learning AirWatch), an active blogger, and has published multiple case studies.

**Tcat Houser** (formerly Tim Catura-Houser) transitioned from vacuum tube (valve) computers in 1965. He got really excited when the Altair got Microsoft BASIC about 1973, because he could have a computer at home. More recently (March 2017), he was surprised with the Presidents award from the [ETA-I.org](http://ETA-I.org) for being a dedicated volunteer.

His career as a global road warrior has included both being a field geek and trainer, only sometimes at his extreme peril. His MCP number 416024 in 2017 marks 20 years as an MCSE.

While some of the titles he has worked on are lost to history, he quit counting after 50 titles. Some of them can be found on Amazon by his former and current name.

Certainly, it is easy for me to say I cannot remember doing a tactical editing project that brought me so many smiles. The author did an amazing job. On the internal side, I

experienced equal pleasure. In my own mind I call it the tale of two Jays. Judie and Juliana at Packt are two astounding individuals! To me, they are more than professional. They are what I would have to call buddies.





# www.PacktPub.com

For support files and downloads related to your book, please visit [www.PacktPub.com](http://www.PacktPub.com).

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at [www.PacktPub.com](http://www.PacktPub.com) and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at [service@packtpub.com](mailto:service@packtpub.com) for more details.

At [www.PacktPub.com](http://www.PacktPub.com), you can also read a collection of free technical articles, sign up for a range of free newsletters and receive exclusive discounts and offers on Packt books and eBooks.



<https://www.packtpub.com/mapt>

Get the most in-demand software skills with Mapt. Mapt gives you full access to all Packt books and video courses, as well as industry-leading tools to help you plan your personal development and advance your career.



# Why subscribe?

- Fully searchable across every book published by Packt
- Copy and paste, print, and bookmark content
- On demand and accessible via a web browser



# Customer Feedback

Thanks for purchasing this Packt book. At Packt, quality is at the heart of our editorial process. To help us improve, please leave us an honest review on this book's Amazon page at <https://www.amazon.com/dp/1787127303>.

If you'd like to join our team of regular reviewers, you can email us at [customerreviews@packtpub.com](mailto:customerreviews@packtpub.com). We award our regular reviewers with free eBooks and videos in exchange for their valuable feedback. Help us be relentless in improving our products!



# Table of Contents

## Preface

What this book covers

What you need for this book

Who this book is for

Conventions

Reader feedback

Customer support

    Downloading the color images of this book

    Errata

    Piracy

    Questions

## 1. Hardware 1.1 (901.1)

    901.1.1 Given a scenario, configure settings, and use BIOS/UEFI tools on a PC

        Firmware upgrades/flash BIOS

        Video training

        Unified Extensible Firmware Infrastructure

        BIOS component information

        BIOS configurations

            Boot sequence

            Enabling and disabling devices

            Date/time

            Clock speeds

            Virtualization support

        BIOS security - passwords, drive encryption - TPM, LoJack, secure boot

            BIOS password

            LoJack

            Secure boot

            Built-in diagnostics

        Monitoring

            Temperature monitoring

            Fan speeds

        Video training

    901.1. 2 Explain the importance of motherboard components, their purpose and properties

        Sizes

            ATX

            NLX (not in exam)

            Micro-ATX

            Mini-ITX

- ITX
- Expansion slots
  - PCI
  - PCI-X
  - Peripheral Component Interconnect Express
  - miniPCI
- RAM slots
  - Rambus Inline Memory Module
  - Synchronous Dynamic RAM
- CPU sockets
  - Chipsets
    - Northbridge
    - Southbridge
  - CMOS battery
  - Power connections and types
  - Fan connectors
  - Data connectors
  - Front/top panel connectors
  - Bus speeds
  - Reset button
- Video training
- 901.1.3 Compare and contrast various RAM types and their features
  - Types
    - DDR
    - DDR2
    - DDR3
    - SODIMM
    - DIMM
    - Parity versus non-parity
    - ECC versus non-ECC
    - RAM configurations
      - Single channel versus dual channel versus triple channel
  - Exam questions
  - Video training
- 901.1.4 Install and configure PC expansion cards
  - Sound cards
  - Video cards
  - Network cards
    - Protocols and services
  - USB cards



FireWire cards

Thunderbolt cards

Storage cards - memory cards

Modem cards

Wireless/cellular cards

TV tuner cards

Video capture cards

Riser cards

Video training

#### 901.1.5 Install and configure storage devices and use appropriate media

Optical drives

CD-ROM/CD-RW

DVD-ROM/DVD-RW/DVD-RW DL

DVD-RW DL

Blu-ray

BD-R

BD-RE

Magnetic hard disk drives

Hot swappable drives

Solid state/flash drives

Compact flash

SD

MicroSD

MiniSD

xD

SSD

Hybrid

eMMC

RAID types

Tape drive

Media capacity

Video training

Summary

## 2. Hardware 1.2 (901.1)

### 901.1.1 Installing various types of CPUs and apply the appropriate cooling methods

Socket types

Characteristics

Speeds

Cores

Cache size/type

- Hyperthreading
- Virtualization support
- Architecture (32-bit versus 64-bit)
- Integrated GPU
- Disable execute bit

#### Cooling

- Heatsink
- Fans
- Thermal paste
- Liquid-based
- Fanless/passive

#### Video training

901.1.2 Comparing and contrasting various PC connection interfaces, their characteristics, and purpose

#### Physical connections

- USB 1 versus 2.0 versus 3.0
- Connector types - B, mini, and micro
- Firewire 400 versus Firewire 800
- SATA1 versus SATA2 versus SATA3, eSATA
- Other connector types
- Wireless connections
- Characteristics of wireless signals

#### Video training

901.1.3 Install a power supply based on given specifications

#### Connector types and their voltages

- SATA
- Molex
- 4/8-pin 12 V
- PCIe 6/8-pin
- 20-pin
- 24-pin

#### Specifications

#### Video training

901.1.4 Given a scenario, select the appropriate components for a custom PC configuration to meet customer specifications or needs

#### Graphic/CAD/CAM design workstation

- Multicore processor
- High-end video
- Maximum RAM

#### Audio/video editing workstation

- Specialized audio and video card
- Large fast hard drive

- Dual monitors
- Virtualization workstation
- Maximum RAM and CPU cores

#### Gaming PC

- Multicore processor
- High-end video/specialized GPU
- High-definition sound card
- High-end cooling

#### Home theatre PC

- Surround sound audio
- HDMI output
- HTPC compact form factor
- TV tuner

#### Standard thick client

- Desktop applications
- Meets recommended requirements for selected OS

#### Thin client

- Basic applications
- Meets minimum requirements for selected OS
- Network connectivity

#### Home server PC

- Media streaming
- File sharing
- Print sharing
- Gigabit NIC
- RAID array

#### Video training

### 901.1.5 Compare and contrast types of display devices and their features

#### LCD

##### TN versus IPS

##### Fluorescent versus LED backlighting

#### Plasma

#### Projector

#### OLED

##### Refresh/frame rates

##### Resolution

##### Native resolution

##### Brightness/lumens

##### Analog versus digital

##### Privacy/anti-glare filters

- Multiple displays
- Aspect ratios
- Video training
- 901.1.6 Identify common PC connector types and associated cables
  - Display connector types
    - Display cable types
  - Device cables and connectors
    - SATA
    - eSATA
    - USB
    - Firewire (IEEE1394)
    - Audio
  - Adapters and converters
    - DVI to HDMI
    - USB A to USB B
    - USB to ethernet
    - DVI to VGA
    - Thunderbolt to DVI
    - PS/2 to USB
    - HDMI to VGA
  - Video training
- 901.1.7 Install and configure common peripheral devices
  - Mouse
  - Keyboard
  - Scanner
  - Barcode reader
  - Biometric devices
  - Game pads
  - Joysticks
  - Digitizer
  - Motion sensor
  - Touchpad
  - Smart card readers
  - Digital cameras
  - Microphone
  - Webcam
  - Camcorder
  - Output devices
    - Printers
    - Speakers

- Display devices
- Input and output devices
  - Touch screen
  - KVM (Keyboard, Video and Mouse)
  - Smart TV
  - Set-top Box
  - MIDI-enabled devices
- Video training

#### Summary

### 3. Hardware 1.3 (901.1)

#### 901.1.1 Installing SOHO multifunction device/printers and configure appropriate settings

- Using appropriate drivers for a given OS

- Configuration settings

- Duplex

- Collate

- Orientation

- Quality

- Device sharing

- Wired

- USB

- Serial

- Ethernet

- Wireless

- Bluetooth

- 802.11 - a/b/g/n/ac

- Infrastructure versus ad hoc

- Integrated print server - hardware

- Cloud printing/remote printing

- Public/shared devices

- Sharing local/networked device via OS settings

- TCP/Bonjour/AirPrint

- Data privacy

- User authentication on the device

- Hard drive caching

- Video training

#### 901.1.2 Comparing and contrasting differences between the various print technologies and the associated imaging process

- Laser

- Inkjet

- Thermal

Impact

Virtual

Print to file

Print to PDF

Print to XPS

Print to image

Video training

901.1.3 Given a scenario, perform appropriate printer maintenance

Laser

Thermal

Impact

Inkjet

Video training

Summary

#### 4. Networking (901.2)

901.2.1 Identify the various types of network cables and connectors

Fiber

Connectors: SC, ST and LC

Twisted pair

Connectors: RJ-11, RJ-45

Wiring standards - T568A and T568B

Coaxial

BNC

F-connector

Exam questions

Video training

901.2.2 Compare and contrast the characteristics of connectors and cabling

Fibre

Speed and transmission limitations

Twisted pair

Speed and transmission limitations

Splitters and effects on signal quality

Coaxial

Speed and transmission limitations

Splitters and the effects on signal quality

Exam questions

Video training

901.2.3 Explain the properties and characteristics of TCP/IP

IPv4 versus IPv6

Legend

Address structure

Address compression

Public versus private versus APIPA/link local

Static versus dynamic

Client-side DNS settings

Client-side DHCP

Subnet mask versus CIDR

Gateway

Exam questions

Video training

#### 901.2.4 Explain common TCP and UDP ports, protocols, and their purpose

Ports

Protocols

DHCP

DNS

LDAP

SNMP

SMB

CIFS

SSH

AFP

TCP versus UDP

Exam questions

Video training

#### 901.2.5 Compare and contrast various Wi-Fi networking standards and encryption types

Standards

802.11 (a/b/g/n/ac)

Speeds, distances, and frequencies:

Encryption types

Exam questions

Video training

#### 901.2.6 Given a scenario, install and configure SOHO wireless/wired router and apply appropriate settings

Channels

Port forwarding, port triggering

DHCP (on/off)

DMZ

NAT/DNAT

Basic QoS

Firmware

UPnP

Exam questions

Video training

#### 901.2.7 Compare and contrast internet connection types, network types and their features

Internet connection types

Cable

DSL

Dial-up

Fiber

Satellite

ISDN

Cellular

Tethering

Mobile hotspot

Line-of-sight wireless Internet service

Network Types

Exam questions

Video training

#### 901.2.8 Compare and contrast network architecture devices, their functions, and their features

Hub

Switch

Router

Access point

Bridge

Modem

Firewall

Patch panel

Repeaters/extenders

Ethernet over power

Power over Ethernet injector

Exam questions

Video training

#### 901.2.9 Given a scenario, use appropriate networking tools

Crimper

Cable stripper

Multimeter

Tone generator and probe

Cable tester

Loopback plug

Punchdown tool

Wi-Fi analyzer



Exam questions

Video training

Summary

## 5. Mobile Devices (901.3)

### 901.3.1 Installing and configuring laptop hardware and components

Expansion options

ExpressCard /34

ExpressCard /54

SODIMM

Flash

Ports/adapters

Thunderbolt

DisplayPort

USB to RJ-45 dongle

USB to Wi-Fi dongle

USB to Bluetooth

USB optical drive

Hardware/device replacement

Keyboard

Hard drive

SSD versus hybrid versus magnetic disk

1.8 inch versus 2.5 inch

Memory

Smart card reader

Optical drive

Wireless card

Mini-PCIe

Screen

DC jack

Battery

Touchpad

Plastics/frames

Speaker

System board

CPU

Video training

### 901.3.2 Explaining the function of components within the display of a laptop

Types

LCD

TN versus IPS

- Fluorescent versus LED backlighting
- OLED
- Wi-Fi antenna connector/placement
- Webcam
- Microphone
- Inverter
- Digitizer
- Video training
- 901.3.3 Given a scenario, use appropriate laptop features
  - Special function keys
  - Video training
- 901.3.4 Explaining the characteristics of various types of other mobile devices
  - Tablets
  - Smartphones
  - Wearable technology devices
    - Smart watches
    - Fitness monitors
    - Glasses and headsets
    - Phablets
    - e-Readers
    - Smart camera
    - GPS
  - Video training
- 901.3.5 Comparing and contrasting accessories and ports of other mobile devices
  - Connection types
    - NFC
    - Proprietary vendor-specific ports (communication/power)
    - MicroUSB/miniUSB
    - Lightning
    - Bluetooth
    - IR
    - Hotspot/tethering
  - Accessories
    - Headsets
    - Game pads
    - Docking stations
    - Extra battery packs/battery chargers
    - Protective covers/water proofing
    - Credit card readers
  - Memory/microSD

Exam questions

Video training

Summary

## 6. Hardware and Network Troubleshooting (901.4)

901.4.1 Given a scenario, troubleshoot common problems related to motherboards, RAM, CPU, and power with appropriate tools

Common symptoms

Unexpected shutdowns

System lockups

POST code beeps

Blank screen on bootup

BIOS time and settings resets

Attempts to boot to incorrect device

Continuous reboots

No power

Overheating

Loud noise

Intermittent device failure

Fans spin - no power to other devices

Indicator lights

Smoke

Burning smell

Proprietary crash screens (BSOD/pin wheel)

Distended capacitors

Tools

Multimeter

Power supply tester

Loopback plugs

POST card/USB

Video training

901.4.2 Given a scenario, troubleshoot hard drives and RAID arrays with appropriate tools

Common symptoms

Read/write failure

Slow performance

Loud clicking noise

Failure to boot

OS not found

Drive not recognized

RAID not found

RAID stops working

Proprietary crash screens (BSOD/pin wheel)

S.M.A.R.T. errors

#### Tools

Screwdriver

External enclosures

CHKDSK

FORMAT

File recovery software

Bootrec

DiskPart

Defragmentation tool

#### Video training

901.4.3 Given a scenario, troubleshoot common video, projector, and display issues

#### Common symptoms

VGA mode

No image on screen

Overheat shutdown

Dead pixels

Artifacts

Color patterns incorrect

Dim image

Flickering image

Distorted image

Distorted geometry

Burn-in

Oversized images and icons

#### Video training

901.4.4 Given a scenario, troubleshoot wired and wireless networks with appropriate tools

#### Common symptoms

No connectivity

APIPA/link local address

Limited connectivity

Local connectivity

Intermittent connectivity

IP conflict

Slow transfer speeds

Low RF signal

SSID not found

#### Hardware tools

Cable tester

- Loopback plug
- Punch-down tools
- Tone generator and probe
- Wire strippers
- Crimper
- Wireless locator
- Command-line tools
  - PING
  - IPCONFIG/IFCONFIG
  - TRACERT
  - NETSTAT
  - NBTSTAT
  - NET
  - NETDOM
  - NSLOOKUP

- Video training

901.4.5 Given a scenario, troubleshoot and repair common mobile device issues while adhering to the appropriate procedures

- Common symptoms

- No display
- Dim display
- Flickering display
- Sticking keys
- Intermittent wireless
- Battery not charging
- Ghost cursor/pointer drift
- No power
- Num lock indicator lights
- No wireless connectivity
- No Bluetooth connectivity
- Cannot display to external monitor
- Touchscreen non-responsive
- Apps not loading
- Slow performance
- Unable to decrypt email
- Extremely short battery life
- Overheating
- Frozen system
- No sound from speakers

- GPS not functioning
- Swollen battery
- Disassembling processes for proper reassembly
  - Document and label cable and screw locations
  - Organizing parts
  - Referring to manufacturer resources
  - Using appropriate hand tools
- Video training
- 901.4.6 Given a scenario, troubleshoot printers with appropriate tools
  - Common symptoms
    - Streaks
    - Faded prints
    - Ghost images
    - Toner not fused to the paper
    - Creased paper
    - Paper not feeding
    - Paper jam
    - No connectivity
    - Garbled characters on paper
    - Vertical lines on page
    - Backed up print queue
    - Low memory errors
    - Access denied
    - Printer will not print
    - Color prints in wrong print color
    - Unable to install printer
    - Error codes
    - Printing blank pages
    - No image on printer display
  - Tools
    - Maintenance kit
    - Toner vacuum
    - Compressed air
    - Printer spooler
  - Exam questions
  - Video training
- Summary
- Next steps
- Introducing part 2 - 220-902

## 7. Windows Operating Systems (902.1)

902.1.1 Comparing and contrasting various features and requirements of Microsoft Operating Systems (Windows Vista, Windows 7, Windows 8, Windows 8.1)

### Features

- 32-bit versus 64-bit
- Aero
- Gadgets
- User Account Control
- BitLocker
- Shadow copy
- System Restore
- ReadyBoost
- Sidebar
- Compatibility mode
- Virtual XP mode
- Windows Easy Transfer (WET)
- Administrative tools
- Windows Defender
- Windows firewall
- Security Center
- Event viewer
- File structure and paths
- Category view versus Classic view
- Side-by-side apps
- Metro UI
- Pinning
- OneDrive
- Windows store
- Multimonitor task bars
- Charms
- Start screen
- PowerShell
- Live sign-in
- Action Center
- Upgrading paths
- Differences between in place upgrades
- Compatibility tools
- Windows upgrade OS advisor

Video training

## 902.1.2 Given a scenario, install Windows PC operating systems using appropriate methods

### Boot methods

USB

CD-ROM

DVD

PXE

Solid state/flash drives

NetBoot

External/hot swappable drive

Internal hard drive (partition)

### Type of installations

Unattended installation

Upgrade

Clean install

Repairing installation

Multiboot

Remote network installation

Image deployment

Recovery partition

Refresh/restore

### Partitioning

Dynamic

Basic

### File system types/formatting

exFAT

FAT32

NTFS

CDFS

NFS

ext3, ext4

Quick format versus full format

Loading alternate third-party drivers when necessary

Workgroup versus domain setup

Time/date/region/language settings

Driver installation, software, and Windows updates

Factory recovery partition

Properly formatted boot drive with the correct partitions/format

Video training

## 902.1.3 Given a scenario, apply appropriate Microsoft command-line tools

Video training



902.1.4 Given a scenario, use appropriate Microsoft operating system features and tools

Administrative

Computer management

Device manager

Local users and groups

Local security policy

Performance monitor

Services

System configuration

Task scheduler

Component services

Data sources

Print management

Windows memory diagnostics

Windows firewall

Advanced security

MSCONFIG

Task Manager

Disk management

Drive status

Mounting

Initializing

Extending partitions

Splitting partitions

Shrink partitions

Assigning/changing drive letters

Adding drives

Adding arrays

Storage spaces

Other tools

System utilities

REGEDIT

COMMAND

SERVICES.MSC

MMC

MSTSC

NOTEPAD

EXPLORER

MSINFO32

DXDIAG

DEFRAG

System Restore

Windows Update

Video training

902.1.5 Given a scenario, use Windows Control Panel utilities

Internet options

Display/display settings

User accounts

Folder options

System

Windows firewall

Power options

Programs and features

HomeGroup

Devices and printers

Sound

Troubleshooting

Network and Sharing Center

Device Manager

Video training

902.1.6 Given a scenario, install and configure Windows networking on a client/desktop

Firewall settings

Configuring an alternative IP address in Windows

Network card properties

Video training

902.1.7 Perform common preventive maintenance procedures using the appropriate Windows OS tools

Best practices

Scheduled backups

Scheduled disk maintenance

Windows updates

Patch management

Driver/firmware updates

Antivirus/anti-malware updates

Tools

Exam questions

Video training

Summary

## 8. Other Operating Systems and Technologies (902.2)

902.2.1 Identifying common features and functionalities of the macOS and Linux operating systems

Best practice techniques with Apple systems

Tools

Features of Apple systems

Basic Linux commands

Video training

902.2.2 Given a scenario, set up, and use client-side virtualization

Purpose of virtual machines/hypervisors

Resource requirements

Emulator requirements

Security requirements

Network requirements

Video training

902.2.3 Identifying basic cloud concepts

Software as a Service

Infrastructure as a Service

Platform as a Service

Public versus private versus hybrid versus community

Rapid elasticity

On-demand

Resource pooling

Measured service

Video training

902.2.4 Summarizing the properties and purpose of services provided by networked Hosts

Server roles

Web server

File server

Print server

DHCP server

DNS server

Proxy server

Mail server

Authentication server

Internet appliance

Unified Threat Management

IDS/IPS

Legacy/embedded systems

Video training

902.2.5 Identifying basic features of mobile operating systems

Android versus iOS versus Windows

Video training

902.2.6 Installing and configuring basic mobile device network connectivity and email

Wireless/cellular data network - enable/disable

Bluetooth

Corporate and ISP email configuration

Integrated commercial provider email configuration

PRI updates/PRL updates/baseband updates

Video training

#### 902.2.7 Summarizing methods and data related to mobile device synchronization

Synchronization methods

Exam questions

Video training

Summary

### 9. Security (902.3)

#### 902.3.1 Identify common security threats and vulnerabilities

Malware

Video training

#### 902.3.2 Compare and contrast common prevention methods

Physical security

Lock doors

Mantrap

Cable locks

Biometrics

ID badges/RFID badge

Key fobs

Smart card

Tokens

Privacy filters

Entry control roster

Digital security

Antivirus/anti-malware

Firewalls

User authentication/strong passwords

Multi factor authentication

Directory permissions, access control lists, and the principle of least privilege

VPN

DLP

Disabling ports

Email filtering

Trusted/untrusted software sources

User education/Acceptable Use Policy (AUP)

Video training

### 902.3.3 Compare and contrast differences of basic Windows OS security settings

- User and groups

- NTFS versus share permissions

- Shared files and folders

- System files and folders

- User authentication and single sign-on

- Run as administrator versus standard user

- Encryption systems

- BitLocker-To-Go

- Video training

### 902.3.4 Given a scenario, deploy, and enforce security best practices to secure a workstation

- Password best practices

  - Setting strong passwords

  - Password expiration

  - Changing default usernames/passwords

  - Screensaver required password

  - BIOS/UEFI passwords and why autorun is disabled

  - Requiring passwords

- Account management

  - Restricting user permissions

  - Login time restrictions

  - Disabling guest account

  - Failed attempts logout

  - Timeout/screen lock

- Patch/update management

- Video training

### 902.3.5 Compare and contrast various methods for securing mobile devices

- Screen locks

  - Fingerprint lock

  - Face lock

  - Swipe lock

  - Passcode lock

- Remote wipes and locator applications

- Remote backup applications

- BYOD versus corporate owned

- Profile security requirements

- Video training

### 902.3.6 Given a scenario, use appropriate data destruction and disposal methods

- Physical destruction

- Recycling or repurposing best practices

Video training

902.3.7 Given a scenario, secure SOHO wireless, and wired networks

Wireless specific

Changing default SSID / Disabling SSID broadcast

Setting encryption

Antenna and access point placement

Radio power levels

Wi-Fi Protected Setup (WPS)

Exam questions

Video training

Summary

## 10. Software Troubleshooting (902.4)

902.4.1 Given a scenario, troubleshoot PC operating system problems with appropriate tools

Common symptoms

Proprietary crash screens (BSOD/pinwheel)

Failure to boot

Improper shutdown

Spontaneous shutdown/restart

Device fails to start/detected

Missing DLL message

Services fails to start

Compatibility error

Slow system performance

Boots to Safe Mode

File fails to open

Missing NTLDR

Missing boot configuration data

Missing operating system

Missing graphical interface

Missing GRUB/LILO

Kernel panic

Graphical Interface fails to load

Multiple monitor misalignment/orientation

Tools

Video training

902.4.2 Given a scenario, troubleshoot common PC security issues with appropriate Tools and best practices

Common symptoms

Tools

Best practice procedure for malware removal

Video training

902.4.3 Given a scenario, troubleshoot common mobile OS and application issues with appropriate tools

Common symptoms

Tools

Video training

902.4.4 Given a scenario, troubleshoot common mobile OS and application security issues with appropriate tools

Common symptoms

Tools

Exam questions

Video training

Summary

## 11. Operational Procedures (902.5)

902.5.1 Given a scenario, use appropriate safety procedures

Equipment grounding

Proper component handling and storage

Toxic waste handling

Personal safety

Electrical fire safety

Cable management

Safety goggles

Compliance with local government regulations /Protection from airborne particles

Video training

902.5.2 Given a scenario with potential environmental impacts, apply the appropriate controls

MSDS documentation for handling and disposal - including Temperature, humidity level awareness, and proper ventilation

Power surges, brownouts, and blackouts

Dust and debris

Compliance to local government regulations

Video training

902.5.3 Summarize the process of addressing prohibited content/activity, and explain privacy, licensing, and policy concepts

Incident response

Licensing/DRM/EULA

Open source versus commercial license

Personal license versus enterprise licenses

Personally Identifiable Information

Following corporate end user policies and security best practices

Video training

902.5.4 Demonstrating proper communication techniques and professionalism

Dealing with difficult customers or situations

Setting and meeting expectations/timeline and communicate status with the customer

Dealing appropriately with customers confidential and private materials

Safeguarding

Video training

902.5.5 Given a scenario, explain the troubleshooting theory

Exam questions

Video training

Summary

Finale

## 12. Processor Table

## 13. Answer Key

Chapter 1: Hardware 1.1 (901.1)

Chapter 4: Networking (901.2)

Chapter 5: Mobile Devices (901.3)

Chapter 6: Hardware and Network Troubleshooting (901.4)

Chapter 7: Windows Operating Systems (902.1)

Chapter 8: Other Operating Systems and Technologies (902.2)

Chapter 9: Security (902.3)

Chapter 10: Software Troubleshooting (902.4)

Chapter 11: Operational Procedures (902.5)





# Preface

The book is divided into two courses. The first course covers content for the CompTIA A+ exam 220-901 and the second covers additional content for the CompTIA A+ 220-902.

In the first course, you will first begin with the understanding and installing CompTIA hardware required for CompTIA A+ 220-901. Next, you will learn to use appropriate networking tools based on different scenarios. Toward the end, you will learn about different domains such as mobile devices, hardware, and network troubleshooting.

In the second course, you will look at how to install and configure an OS on a client/desktop, covering a range of mobile and network devices and platforms. We will perform common preventive maintenance procedures using the appropriate Windows OS tools and you will also learn to perform the same tasks with other OSes.

Finally, you will learn about security best practices to secure a workstation and also troubleshoot any system and OS issues, application issues, or security issues.

To download the Exam Objectives for CompTIA, please refer to the following link:

<https://certification.comptia.org/certifications/a>

The exam questions for [Chapter 2](#), Hardware 1.2 (901.1) and [Chapter 3](#), Hardware 1.3 (901.1) is covered in [Chapter 1](#), Hardware 1.1 (901.1).



# What this book covers

[Chapter 1](#), Hardware 1.1 (901.1), introduces you to the main usage of the A+ certification and how to identify hardware components found within any type of system.

[Chapter 2](#), Hardware 1.2 (901.1), walks you through processors, connectors, ports, and display outputs. We will then look at bespoke systems, for example, Highend Rich Media Video Editing systems or Graphics Rendering stations to see how their requirements exceed normal expectations.

[Chapter 3](#), Hardware 1.3 (901.1), describes imaging and interaction on the periphery of the system by focusing on document imaging and scanning, that is, input and output to external documents and sources.

[Chapter 4](#), Networking (901.2), focuses on how systems or other end-user devices can communicate with other devices on the network using the Open Systems Interconnection (OSI) model. This model is used in network design and troubleshooting to establish at what level within the network a problem may be occurring.

[Chapter 5](#), Mobile Devices (901.3), starts by attaching storage and additional functionality to mobile devices that are unique to laptops. We will then look at the internal hardware specific to laptops.

[Chapter 6](#), Hardware and Network Troubleshooting (901.4), discusses the common problems you will encounter within a system. You will start by concentrating on symptoms common to an individual system, and these could affect any type or style of system. By the end, we will learn how to solve these issues.

[Chapter 7](#), Windows Operating Systems (902.1), provides the first look at the Windows systems from Vista to Windows 10. We then focus specifically on the Control Panel toolset, specific network elements, and then finally maintenance procedures specific to Windows.

[Chapter 8](#), Other Operating Systems and Technologies (902.2), caters not only to Microsoft systems but other systems as well. We will learn Microsoft systems first and then this will give us a context for the other operating systems, such as macOS and Linux, which are in fact very similar.

[Chapter 9](#), Security (902.3), categorizes each of the different attacks we might expect to encounter on an enterprise network, looking at their severity and how they affect the network.

[Chapter 10](#), Software Troubleshooting (902.4), helps us to fix things that will go wrong, or be misconfigured due to hardware age and software updates, while having a great network system.

[Chapter 11](#), Operational Procedures (902.5), covers the safety of the equipment and its users. We will consider environmental safety aspects and policies, and then look at broader information security policies used to ensure organizational safety.

[Appendix A](#), Processor Table, covers the type of processors that are available for recent systems, their technologies, how to install them, and how to troubleshoot them.

[Appendix B](#), Answer Key, provides you with the answers to all the question sets that are given in each chapter.



# What you need for this book

Any hardware/software is advisory only and not a mandatory requirement. You should be able to access a working system to install Windows Vista or later. You need to know Windows 7 and 8 (mandatory for the 902 exam) and be able to access Linux as well. Online lab access for these is fine.

There are links in the book to TechNet, where you can get the evaluation copies of Windows client and server. Also, the Ubuntu page will be good for Linux. Apple is proprietary, so it is harder to access them and CompTIA does not make it mandatory because they cannot force people to buy the Apple kit for the exam.

Knowledge of iPhone and Android phones is needed for 902 and there is a presumption that you have access to these.

Regarding network switches/routers, you have links to the online simulations (such as Linksys). Cisco is mentioned in passing but there is no requirement to have access to the Cisco kit.





# Who this book is for

This book is aimed at people who have interest in a career in the IT industry, but currently, have little or no practical experience to attest to your skills. Most of our delegates go on to work as first-line IT technicians, and from this point establish a career through the organizational structure to later specialize in specific IT technologies. However, you're not ready for that yet.

With your screwdriver in one hand and the book in the other, let's get you to a position where you can prove that you are both confident and competent.



# Conventions

In this book, you will find a number of text styles that distinguish between different kinds of information. Here are some examples of these styles and an explanation of their meaning. Code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles are shown as follows: "An example IPv6 address is: 2001:0bc2:25d2:0000:0000:8bbd:0261:6231".

Any command-line input or output is written as follows:

```
dsadd user "cn=John Smith,ou=SouthEmployees,  
dc=northwindtraders,dc=com" -disabled no -pwd C^h3Bdo9#  
-mustchpwd yes
```

**New terms** and **important words** are shown in bold. Words that you see on the screen, for example, in menus or dialog boxes, appear in the text like this: " The Previous Versions tab was removed in Windows 8, but restored in 10. "



Warnings or important notes appear like this.



Tips and tricks appear like this.



# Reader feedback

Feedback from our readers is always welcome. Let us know what you think about this book-what you liked or disliked. Reader feedback is important for us as it helps us develop titles that you will really get the most out of. To send us general feedback, simply email [feedback@packtpub.com](mailto:feedback@packtpub.com), and mention the book's title in the subject of your message. If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, see our author guide at [www.packtpub.com/authors](http://www.packtpub.com/authors).



# Customer support

Now that you are the proud owner of a Packt book, we have a number of things to help you to get the most from your purchase.





# Downloading the color images of this book

We also provide you with a PDF file that has color images of the screenshots/diagrams used in this book. The color images will help you better understand the changes in the output. You can download this file from [https://www.packtpub.com/sites/default/files/downloads/CompTIA+CertificationGuide\(220-901and220-902\)\\_ColorImages.pdf](https://www.packtpub.com/sites/default/files/downloads/CompTIA+CertificationGuide(220-901and220-902)_ColorImages.pdf).



# Errata

Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you find a mistake in one of our books-maybe a mistake in the text or the code-we would be grateful if you could report this to us. By doing so, you can save other readers from frustration and help us improve subsequent versions of this book. If you find any errata, please report them by visiting <http://www.packtpub.com/submit-errata>, selecting your book, clicking on the Errata Submission Form link, and entering the details of your errata. Once your errata are verified, your submission will be accepted and the errata will be uploaded to our website or added to any list of existing errata under the Errata section of that title. To view the previously submitted errata, go to <https://www.packtpub.com/books/content/support> and enter the name of the book in the search field. The required information will appear under the Errata section.



# Piracy

Piracy of copyrighted material on the internet is an ongoing problem across all media. At Packt, we take the protection of our copyright and licenses very seriously. If you come across any illegal copies of our works in any form on the internet, please provide us with the location address or website name immediately so that we can pursue a remedy. Please contact us at [copyright@packtpub.com](mailto:copyright@packtpub.com) with a link to the suspected pirated material. We appreciate your help in protecting our authors and our ability to bring you valuable content.



# Questions

If you have a problem with any aspect of this book, you can contact us at [questions@packtpub.com](mailto:questions@packtpub.com), and we will do our best to address the problem.





# Hardware 1.1 (901.1)

This chapter focuses on the main usage of the A+ certification--how to identify hardware components found within any type of computer. Contextualize these and learn how components have changed over time. Learn which component type is more recent or more powerful than another. Determine which hardware components are associated with which manufacturer or type of computer system.

In this chapter, we will be looking at a large amount of facts and figures you will have to remember for the exam. We will be contextualizing over 30 years of ICT information, so it will be helpful to you if you determine a timeline of changes and mentally categorize and group similar hardware together to understand how one component has changed and enhanced over time.

This is a large and very important section of the 901 exam. We have split the first module into three chapters, given its size. Across these chapters we will cover the following concepts:

- Given a scenario, configure settings and use BIOS/UEFI tools on a PC.
- Explain the importance of motherboard components, their purpose and properties.
- Compare and contrast various RAM types and their features.
- Install and configure PC expansion cards. Install and configure storage devices and use appropriate media.
- Install various types of CPUs and apply the appropriate cooling methods.
- Compare and contrast various PC connection interfaces, their characteristics and purpose.
- Install a power supply based on given specifications.
- Given a scenario, select the appropriate components for a custom PC configuration to meet customer specifications or needs.
- Compare and contrast types of display devices and their features.
- Identify common PC connector types and associated cables.
- Install and configure common peripheral devices.
- Install SOHO multifunction device/printers and configure appropriate settings.
- Compare and contrast differences between the various print technologies and the associated imaging process.
- Given a scenario, perform appropriate printer maintenance.





# **901.1.1 Given a scenario, configure settings, and use BIOS/UEFI tools on a PC**

This first section is absolutely chock full of detail. Here, we start with possibly the most important part of the A+ course -- we consider at the electronic level what a computer is and some of the key components to making it work. We start with the concept of the BIOS and how this can be kept up to date. We then consider some of the custom settings held by the BIOS and how the BIOS helps to determine the speed the computer will run at, as well as how it will load. We look at some of the built-in self-testing that takes place, and also how the machine monitors itself and makes decisions based on changes in voltage and temperature of components.

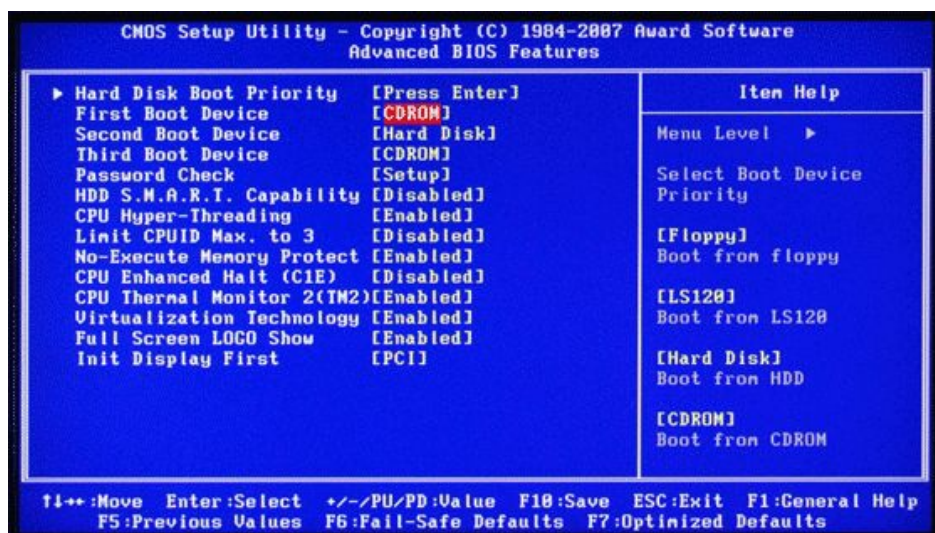


# Firmware upgrades/flash BIOS

Contained on the motherboard, the heart and brain of the computer system is a silicon chip, which was programmed at the factory. It retains its core operating system even when the power is switched off due to the nature of the chip. This carbon metal oxide semiconductor contains a series of menus and configuration settings, which are responsible for managing the power and speed of the processor, integrating with the on-board memory or **Random Access Memory (RAM)**. The **Basic Input Output System (BIOS)** for short, is a protected menu, it is not easy to get into and therefore most end-users will not be aware of its existence, but the key is that information from the BIOS determines how the computer works with its neighboring components, which data drive to boot into to find the main Operating System (for example, Apple OS X) and if certain additional features new to the motherboard can or should be used.

As with most things in the IT world, the terms CMOS and BIOS are interchangeable and are both used to refer to the same thing. However, in truth the CMOS is the physical chip where the BIOS software resides. We do, however, refer to both as either CMOS or BIOS, and this is normal.

There are two key manufacturers for modern PCs--**American Megatrends' AMI BIOS** and **Award's BIOS**:

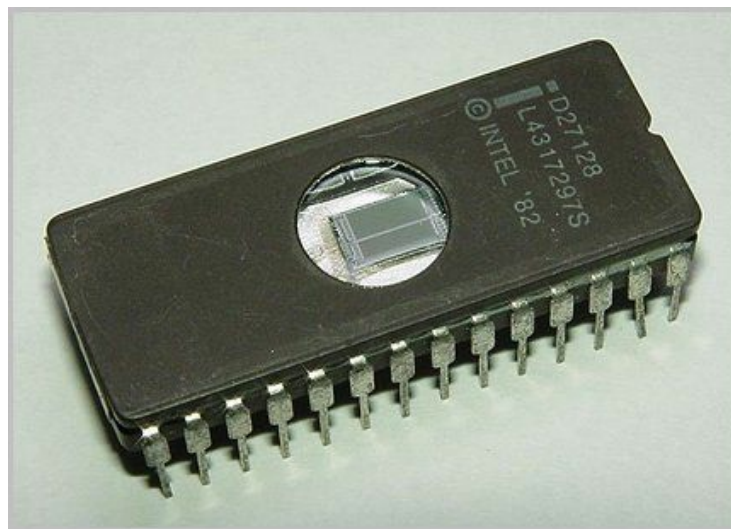


An AWARD BIOS screen

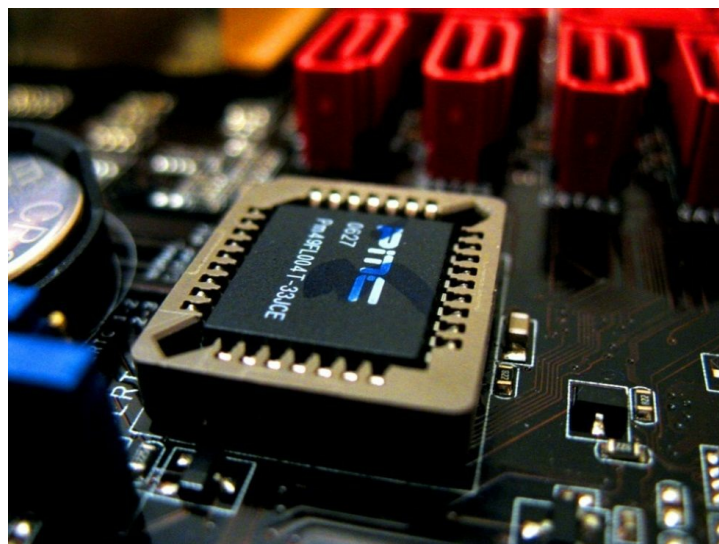
As software updates over time the functionality of the physical hardware also needs to ensure that it can support these changes. For example, a Wi-Fi card may not be aware of

a new protocol, which has recently come onto the market; however, to support it additional parameters may need to be set in the BIOS software, which were not present in the software when the motherboard was first released. To update the motherboard, we need to reprogram it using flashing software. There is a story attached to this original **Electrically Programmable Read Only Memory (EPROM)** chips had to be programmed in the factory, in low-level machine code, and could not be altered by the end user. Later versions were **Erasable and Electrically Programmable ROM (EEPROM)**. These had different techniques to clear data stored on the chip, but typically you had to reset it by passing an electrical current across the chip by using a special **jumper** found on the motherboard, which clears the chip.

On even earlier models, you had to shine ultraviolet light through the observation window at the top of the chip to clear the data, before then reprogramming it:



An early EPROM chip with viewing port



Reprogramming required either a controller card and a low-level program, or by uploading a binary file onto the chip using dedicated software. However, the process of reprogramming this chip is extremely dangerous, if the power supply is cut while the data is being stored onto the chip the process cannot be repeated, so the motherboard cannot be recovered. This will make for a very expensive paperweight!

To upgrade the BIOS software the process is as follows:

- Visit the manufacturer's website and research if your motherboard version is supported by the latest BIOS update. If not, there is no need to update the BIOS and doing so will render the motherboard unusable.
- From the website, download a digitally signed binary file with a version number supported by your motherboard. A **digital signature** is your guarantee that the file you are downloading is legitimate and has not been altered by a third party.
- The binary file needs a special application to communicate with the CMOS. The OS typically does not have the facility to write to the CMOS file, so this application needs to be installed first:



Dell BIOS firmware update

**Exam tip:** In the scenario you are being presented with, is flashing the BIOS safe? Is there a better solution? BIOS updates should be seen as a last resort and are usually done at the very start of a PC build, as part of the hardening process where security is tightened and updates are added.





**Scenario:** You have purchased a standard integrated motherboard for a new system you are in the process of building. You have checked the manufacturer's website and notice that the board is still supported and has several new features, but the version of the board you have purchased has been on the shelf for two years. When you build the system you notice that the integrated Wi-Fi card only supports 802.11a and 802.11b, but not g or n, although the hardware physically supports it. What would you do to render the board more usable?

### Do I know this?

- A digitally signed binary file from the manufacturer
- An update tool from the manufacturer, which will work on your current OS

Smartphones have a similar functionality. Most have a reserve base OS with a secret key combination that allows you to enter **admin mode**. Here, you can clear the main drive and re-install the factory default version of the OS image.

For example, on Android smartphones:

- From power off, with the VOLUME UP key held down, press and hold the POWER button until the Fastboot screen appears
- Use the VOLUME DOWN to scroll to RECOVERY and tap the POWER button to select
- When Android and a red exclamation mark appear, quickly press VOLUME UP and the POWER button at the same time
- Use the VOLUME DOWN button to scroll, to wipe data/factory reset and tap the POWER button to select
- When the wipe is complete use the POWER button to select reboot system now:



An Android Smartphone FASTBOOT screen



# Video training

<http://www.professormesser.com/free-a-plus-training/220-901/bios-and-uefi/>



# Unified Extensible Firmware Infrastructure

**Unified Extensible Firmware Infrastructure (UEFI)** is designed to be a replacement to the BIOS. It supports further security, remote diagnostics, and computer repair without the need of an Operating System being present. With UEFI we can also save a pre-loaded Operating System so that when the PC is restarted we boot directly back into a working system within a matter of seconds, data relating to the drivers, hardware, and OS architecture has already been loaded when the data stored in RAM is saved as a **UEFI boot**. UEFI also supports Bitlocker and has become very important to companies, as we have faced in the past few years a growing number of viruses designed to attack the BIOS and lowest level of the installed OS.

If the user can be tricked into thinking that the BIOS binary update is genuine, then they may decide to update the BIOS with a binary file that is not digitally signed, and as part of the update will end up installing a damaging virus at the BIOS level. UEFI acts as a protection boundary and replacement for the BIOS.



# BIOS component information

So I've introduced the BIOS as a very important, but basic Operating System which helps the system to control the hardware which makes up the key components. Let's look at some of these key areas.

- **RAM:** BIOS performs a RAM test to determine the size of available RAM.
- **Hard drive:** The BIOS menu supports changes to key areas of the system. It performs a disk check to find all drives available to it. Each drive is determined by sending a **handshake signal** onto the IDE, ATA, or SCSI cables and listing the **found** drives.
- **Optical drive:** Systems support the booting of an operating system by both optical drive or a USB drive. Typically, the network administrator uses a separate CD/ISO which will bypass the OS and in fact be loaded first to make changes to the main **host** operating system without the need to load it. For example, if I wanted to copy a system partition on which the OS is installed, I cannot access all of the files within that partition when those files are in use by the OS. To bypass this, we load a different OS from a removable drive and use this to make the necessary changes.
- **CPU:** The BIOS determines the speed of data flow into the CPU and ensures a consistent **clock speed**, ensuring that all devices communicate at the correct speed and are in synchronization.





# BIOS configurations

As we go through the various menu pages there are several key tasks we need to perform before you should consider installing the Operating System.



# Boot sequence

The BIOS supports a **boot order** so that if the OS boot files are not discovered on the first drive, the BIOS instructs the system where to look next, for example, onto an optical drive.



# Enabling and disabling devices

The motherboard is modularized and contains several built-in components such as an on-board sound card, video card, Wi-Fi card, and NIC. Although it is good to have these in that it simplifies the PC build, the on-board components are typically basic. If you have, for example, purchased a high-end graphics card for gaming purposes as the built-in graphics card is not up to the job, you can disable the on-board graphics card and thereby free up system resources and avoid system conflicts or leave both video display adapters running and can then extend your desktop.



# Date/time

The motherboard contains a crystal clock powered by a lithium battery similar to those used for wristwatches. Once the time and date are set in the BIOS, the clock time will continue to count even with the system is switched off. The lithium battery provides residual power to keep the clock running.

Regarding the date/time setting, if the computer is connected to a network a timestamp is sent with any instructions sent to other computers or servers across the network. If the PC is part of a domain, the domain controller is responsible for keeping a computer object within the **Active Directory (AD)** database that relates to your computer. The domain controller also tracks communication with a date stamp. If your computer is out of synchronization to the domain controller for more than 10 minutes, then your computer will fall out of trust and no longer be considered part of the domain. The time will need to be brought back up to date and the PC either rejoined to the domain, or the computer object in AD be reset (on Server 2012 or 2016 systems).

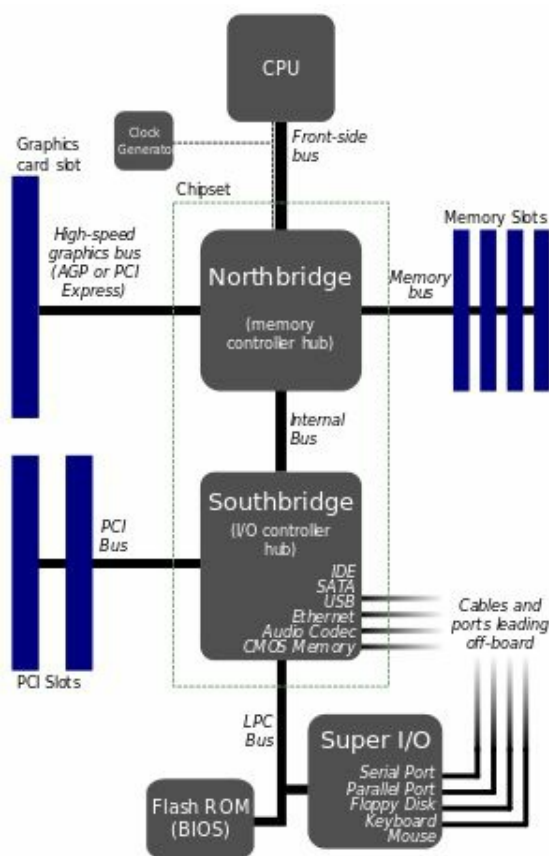
**Scenario--**You have a PC that does not keep the date and time. How do you fix this? If the power provided by the lithium battery is too low because the battery has worn down over time, replace the battery.





# Clock speeds

The **Front-side bus** refers to the speed in MHz the motherboard uses to communicate to the processor and RAM. The **Back-side bus** refers to a multiple of this number used to communicate with the other external components. The **Back-side bus** used a memory buffer referred to as the level two cache. This used to be a separate chip located on the motherboard, but more recently this buffer has been integrated into the processor itself. However, it is still good to think of the design of the PC as being front side and back side:

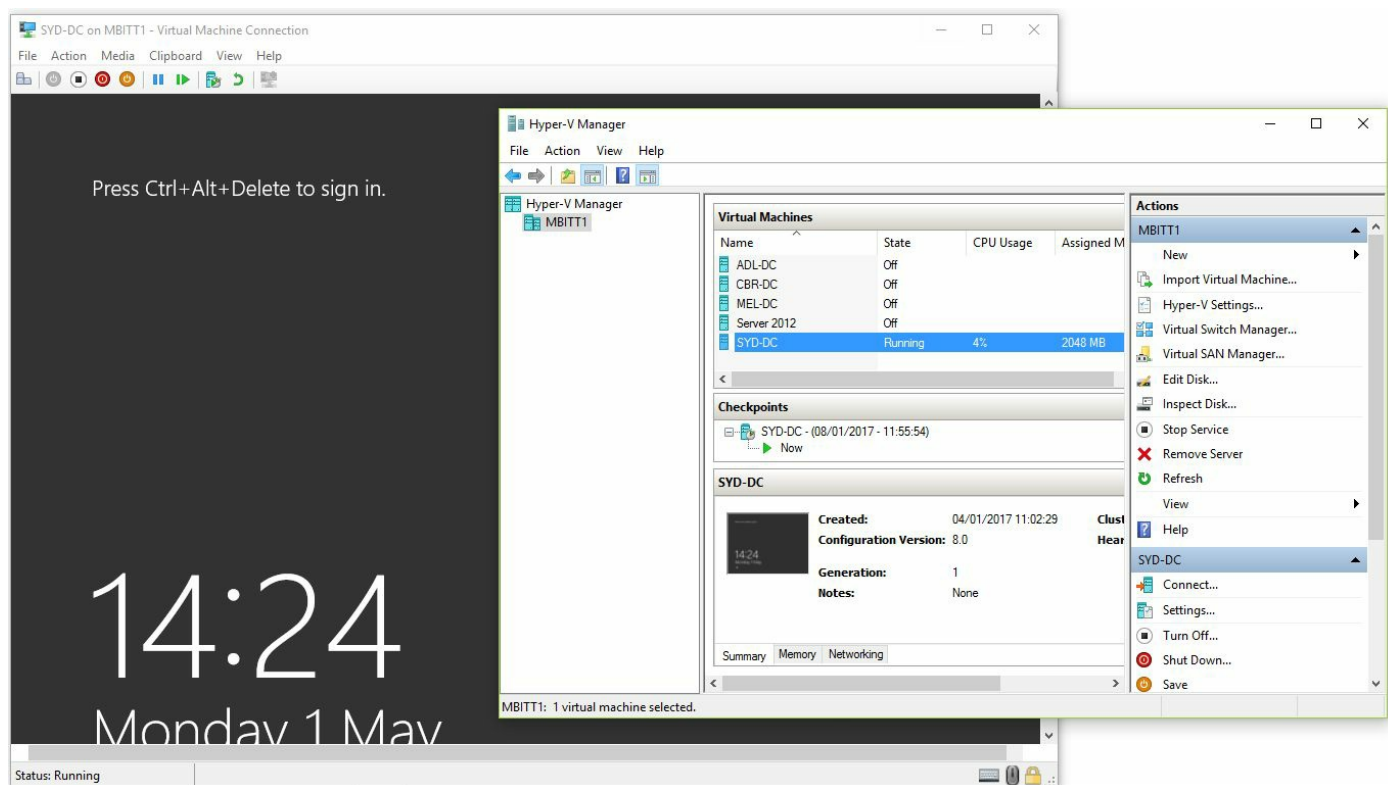


PC system bus architecture



# Virtualization support

Enabling hardware virtualization in the BIOS allows a hypervisor such as Microsoft's Hyper-V to make use of the processor as if the virtual machine were a physical machine. Without this setting, virtual machines are emulated and do not share physical resources:



A Windows 10 client with Hyper-V also running a virtualised Virtual Machine with Windows Server 2012 R2 loaded



# **BIOS security - passwords, drive encryption - TPM, LoJack, secure boot**

As well as performing typical tasks to get the best out of the system we need to protect it. This section will look at security settings and also hint to the replacement BIOS covered in more detail later on in the book--UEFI:



# BIOS password

Given that, from the BIOS, security on the PC can be undone, it is sensible to lock the BIOS from unplanned changes by the end user by assigning an administrator password. On a corporate network this password is typically the same for all client machines.

The BIOS/UEFI can also encrypt portions of the hard drive and protect these with an encryption key stored in a separate chip referred to as the **Trusted Platform Module (TPM)** chip. Its data is encrypted and the encryption/decryption key is stored on the TPM chip, on the motherboard. This ensures that data stored within the UEFI system is not easy to access and alter.





# LoJack

This is a system built into most modern devices such as car radios, smartphones, and laptops. It is a geolocation transmitter device built into the device itself. It does not need an OS to be present to work, but in the event of the device going LoJack GPS, Wi-Fi, or IP geolocation can be used to either track or remote-wipe data from the device. It is typically used by the police to locate stolen items, but can also be used by mobile phone providers to locate or remote-wipe a phone.



# Secure boot

Over the past five years, recent attempts to hack a system have included more sophisticated viruses aimed at damaging the root (the core) of the OS, known as **rootkits**. It is therefore important that the integrity of the OS is protected. This is achieved by encrypting the drivers used to load the system. These are stored in an encrypted fashion and the encryption/decryption key is a file stored within the TPM chip and accessed by UEFI during the startup process. Drivers and key files used to start the system are accessed and decrypted. The encryption key used is created by the OS when UEFI secure boot is first triggered. This is specific to the computer and can only be used on this computer as the ID information from the hardware which makes up this computer forms part of the key itself. Once this **Platform Key** has been created, each driver is encrypted with the Platform Key.



Secure boot is a cross-platform technology. It is supported from Windows 8 and higher, Linux Fedora since v18, OpenSUSE (since v12.3) RHEL 7, CENTOS 7, and Ubuntu v12.04.2.

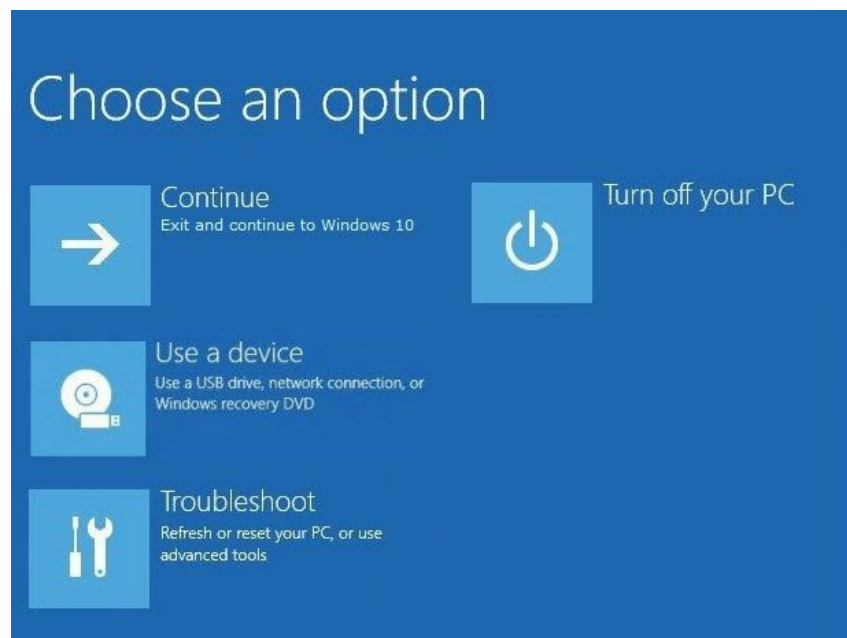


# Built-in diagnostics

Windows and Android systems are good examples of this. An OS is quite modular, each section of it is governed by hundreds of files, which together form the OS. Files are loaded depending on how the OS is structured and the hardware it has to work with. Each driver is loaded from a list of required drivers and is tested to ensure that each is working. Some of these files are considered to be **core** or **critical**, meaning that without them the OS is not capable of working.

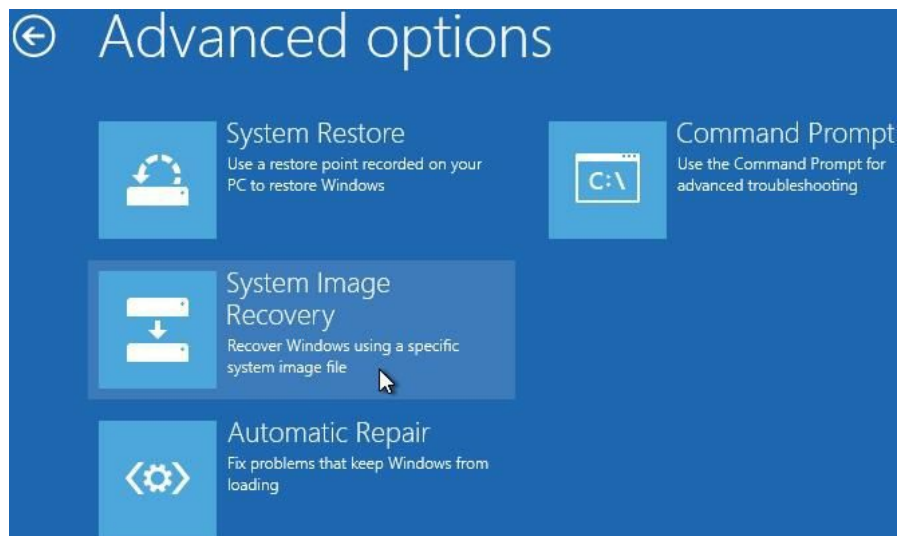
Modern OS systems store a cache of core files and are able to perform a self-repair should one of these core files become corrupted or deleted. If the file is not located, this will trigger a **maintenance mode**, prompting the user to either refresh or reset the device.

This first slide shows the main menu for the F8 Advanced Boot Menu on Windows 8+ systems:



Windows 10 table showing the Windows Recovery Environment

This slide shows the second screen where you can select Automatic Repair, of the refresh/restore options on Windows 8+ systems:



Windows RE advanced Recovery screen





# Monitoring

There are a variety of sensors built into the chassis and motherboard feeding back data to the BIOS and then in turn to the OS. Some of these are significant for different reasons.



# Temperature monitoring

A server is typically **headless**. This means that it is mounted into an enclosure such as a rack-mounted blade server, which has its own closed environment and an air-conditioning unit channeling air into hot and cold zones. The cold air is pushed through and into the computer chassis from the front of the blade server, where the air heats up as it passes over the heatsink. The now-hot air is exhausted from the rear of the blade where it is channeled back into the air-conditioning unit and recycled. Should the temperature get too high, the OS is designed to shut the server down gracefully.

**Exam question--** You discover a cabinet-enclosed server constantly resetting and throttling (running slowly). What has caused this and how can it be resolved? Here, the answer is to identify that there is a buildup of heat caused either by an improperly designed enclosure, or a chassis/heat sink fan not working causing a hotspot.



# Fan speeds

If a fan is not working at all, or at too low a speed to be effective, then temperature will build up on the component causing a hotspot. If the measured temperature (for example, of the CPU) reaches a critical level defined within the OS software, then the machine will automatically shut down so that the CPU can cool down and will not burn out. If the temperature can be reduced two methods are used. First, additional processing loads to the CPU are stopped and if possible redeployed to other **healthy** CPUs. This process is referred to as throttling. If the CPU fan speed can be increased then the increase in airflow will ensure quicker exhaust of the heated air, which will also slowly reduce the CPU temperature.

**Intrusion detection/notification**--A trigger switch is present within the chassis, if the switch has been triggered through the process of opening the inspection plate on the side of the PC enclosure, a log is noted in the BIOS and sent to the OS event log that there has been a physical intrusion:

- Voltage
- Clock
- Bus speed

Together, the voltage, clock frequency, clock multiplier, and bus speed form the processor speed we now measure in GHz. By altering these metrics we can obtain up to a maximum processor speed for that particular processor. Many motherboards are generic and support different types of processor, so it is important when building a PC that the correct values, as stated in the processor installation guide, are used.

The process of deliberately using a processor at a rating under the value it was designed to run at will reduce energy consumption and possibly improve the life of the CPU, but the process was designed to run at an optimal speed:



An overclocked PC showing the CPU-Z and CPU Speed apps

The process of running the CPU at values higher than those recommended by the manufacturer is referred to as **overclocking**. This was popular in the 1990s, but is now considered bad practice. Overclocking the processor increases the likelihood of data errors, heat buildup, system resets, and of course significantly reduces the life of the processor.

Monitoring software will also report back on the current voltage, clock frequency, and bus speed.



# Video training

- **BIOS and UEFI (7:30):** (<http://www.professormesser.com/?p=19295>)
- **BIOS Configuration (6:03):** (<http://www.professormesser.com/?p=19300>)
- **BIOS Security (5:00):** (<http://www.professormesser.com/?p=19304>)
- **Installing BIOS Upgrades (7:05):** (<http://www.professormesser.com/?p=19309>)





# 901.1. 2 Explain the importance of motherboard components, their purpose and properties

What does a computer look like? There is in fact a very easy answer to this--the original standard was the early IBM Desktop PC from 1986. It had a large metal box as a chassis, disk drives within, and a monitor placed on top. That particular dimension of PC, and more importantly of the motherboard housed within the chassis, has become our benchmark. From this, derivations of motherboard size have been developed to accommodate different situations and uses. These have led to fewer, or different, internal ports, which are also discussed here.

In this section, we detail all of the components which makes up the **mainboard** or **motherboard**. We consider the use and purpose of each component and how it all fits together.



# Sizes

The typical PC chassis is universal, accepting a range of form factors, that is, the physical dimension of the motherboard. Screw holes for **spacers** used to hold the motherboard in stasis above the metal chassis (thereby avoiding electric shocks and shorts) have been pre-drilled into the side of the casing and motherboard sizes are common standards so that some of the same drill holes appear in the same place on most boards:



Motherboard size comparison chart

The AT board shipped with the original IBM PCs used in 1985. However, there was a design flaw--graphics cards back then were lengthy, stretching to approximately 30 cm across. The **Northbridge** part of the board's circuitry was designed in such a way that the video card often overlapped the RAM slots. The original **Full AT's** size was 13.8 × 12 inches (351 × 305 mm).



# ATX

The solution to the above problem was to turn the Northbridge section of the board's circuitry around by 90 degrees, thereby freeing space for the graphics card and RAM, which now sits higher on the board. The **ATX** board was released in 1995 and has a size of  $12 \times 9.6$  in ( $305 \times 244$  mm).



# NLX (not in exam)

The **NLX** board was made to be deliberately larger than the ATX to support servers with multiple processors on the board. You wanted the components to be spaced apart to allow for good airflow. Typical NLX sizes range from  $10 \times 8$  in ( $254 \times 203$  mm) to  $13.6 \times 9$  in ( $345 \times 229$  mm). These can only be found in a blade server or standalone server chassis.





# Micro-ATX

This became the standard for home users from 1997 and allowed for smaller chassis. It is 25 percent smaller than the ATX standard at  $9.6 \times 9.6$  in ( $244 \times 244$  mm).



# Mini-ITX

These boards were developed in 2001 for use in home media center systems and other standalone dedicated boxes where power consumption would be less than a typical PC. Clearly there is a limit on the ports available on such a card as it is intended to serve one dedicated purpose. They remain popular due to their small size, low noise, and smaller power consumption. The board size is  $6.7 \times 6.7$  in ( $170 \times 170$  mm).



# ITX

As a standard, the comparison between ATX and ITX is that the ATX is quite generic can be built for various purposes, whereas the ITX is built with a specific purpose in mind. As the size diminishes, chassis are built for the board rather than creating boards that will fit within a universal chassis. ITX is all about integration, so cable management and airflow are more significant and the build will take longer than with ATX.

For smartphones, we use the Mobile-ITX form factor. There is very little space in the chassis, which is molded to fit the board, which has a size of  $3.0 \times 901.1.8$  in ( $75 \times 45$  mm).



The Raspberry Pi (original) has a proprietary form factor and size of  $3.370$  in  $\times$   $2.224$  in ( $85.60$  mm  $\times$   $56.5$  mm)

Remember: I for Integrated.



Standard-ATX



Micro-ATX



Mini-ITX



Nano-ITX



Pico-ITX

Board Form Factor comparisons



# Expansion slots

An expansion slot is a connector found typically on the southern section of the motherboard. These allow for additional devices to connect to the motherboard and enable further functionality not offered by the motherboard. For example, some early motherboards did not have an integrated NIC, so it was necessary to purchase this separately and connect it via an expansion slot.

The earliest internal connector used was the **Industry Standard Architecture (ISA)** slot. These were available on the original PCs in 1986, with a connection bandwidth of 8 or 16 bits, but were extremely slow by today's standards. We will focus on their replacement types.





# PCI

Conventional **Peripheral Component Interconnect (PCI)** is now the common bus standard. It was introduced in 1992. Communication bandwidth is either 32 or 64-bit and speeds from 133 MB/s (32-bit at 33 MHz - the standard configuration), 266 MB/s (32-bit at 66 MHz or 64-bit at 33 MHz), and 533 MB/s (64-bit at 66 MHz) can be achieved.



# PCI-X

**PCI Extended** was designed with servers in mind. Its modified command language supports speeds of 1064 MB/s, making it highly useful for RAID disk transfers using SCSI. The bus transfer system was more elegant, once the data has been sent, the sender disconnects from the data bus allowing other devices to use the bus. Error correcting became a selling point for server motherboards containing PCI-X. This makes the system more efficient than standard PCI, which did not do this.



# Peripheral Component Interconnect Express

**Peripheral Component Interconnect Express (PCIe)** is a serial standard. Where PCI was parallel and shared several devices across one data bus, here only one device connects using one PCIe-dedicated bus. The PCIe data transfer was fast, with little wait time (latency) as compared to PCI. Data is transferred over two signal pairs: two wires for transmitting and two wires for receiving. Each set of signal pairs is called a **lane**, and each lane is capable of sending and receiving 8-bit data packets simultaneously. We then use 1, 2, 4, 8, 16, or 32 lanes depending on the capability of the connecting peripheral.

PCIe and AGP systems talked directly to the Northbridge bypassing the traditional PCI bus:

PCIe architecture	Raw bit rate	Bandwidth per lane direction	Total bandwidth for x16 link
PCIe 901.1.x	2.5GT/s	~250MB/s	~ 8GB/s
PCIe 2.0	5.0GT/s	~500MB/s	~ 16GB/s
PCIe 3.0	8.0GT/s	~1GB/s	~ 32GB/s

## PCI Express 901.1.x bandwidth:



x1 Lane = 2.5 GT/s (2.5 Gbps) @ 8b/10b encoding--250MB/s per differential pair

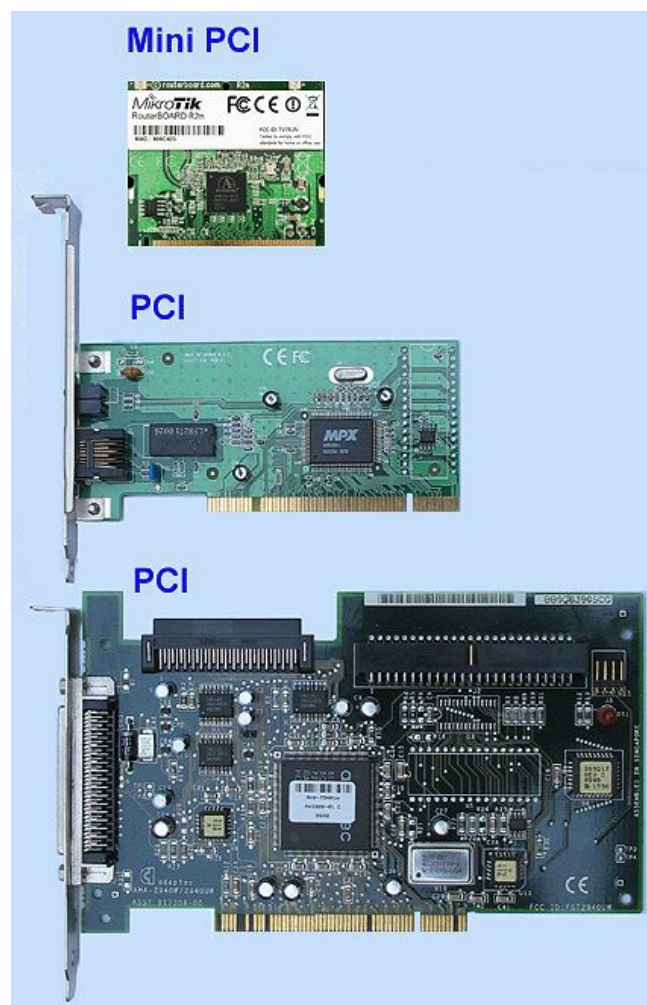
x16 Lane = 16 x 250MB/s per direction = 4GB/s (8GB/s Duplex)



# miniPCI

At 3.3 volts and a bandwidth of 32 bits, miniPCI can be found in laptops, DVD players, HDTVs, and other proprietary devices where the system size is quite small.

There are three types of miniPCI. Types 1 and 2 have 100 connecting pins. Type 3 has 124 pins. You will notice that Type 2 cards are also thick enough that the card side containing the ports and connectors viewable from the outside of the chassis can support an RJ45 network port. Type 1 and Type 3 cards, however, do not--these are thinner and cannot support the width of a network port:



PCI and MiniPCI cards





# RAM slots

Typically, there are four slots on a standard motherboard. These are typically color-coded to signify that it is a dual-channel system. To get the performance of dual-channel, data can be written to both RAM cards, which make up the dual channel at the same time. For example, if I install 4 x 4 GB RAM sticks then I will have 8 GB written to at the same time on one channel, then a further 8 GB written to on the second channel. This is further broken down so that a total of 16 GB could potentially be written to the RAM slots at 4 GB each stick at the same time.

The CompTIA A+ makes little mention now of **Single Inline Memory Module (SIMM)**, SDRAM (the concept), or RIMM. For historical purposes, they are explained here-- SIMM means that the contacts on either side of the memory module (the card) operate separately to each other. A steel clip at either side of the stick held the RAM in place. On a **Dual Inline Memory Module (DIMM)** system, the chips on both sides form one bank (akin to a cassette tape - side A and side B together form the album). SIMMs were finally phased out in the late 1990s:



SIMM RAM from 1990



# Rambus Inline Memory Module

**Rambus Inline Memory Module (RIMM)** were designed by Kingston Technology, who made a high-performance SDRAM contained within its own heatsink, which made them more robust. RIMM had to be added in pairs for the channel to work so, where all of the chips were on one module, a blank stick referred to as a **Continuation RIMM (CRIMM)** was added.

The Sony PlayStation 2 gaming system used RIMM memory:

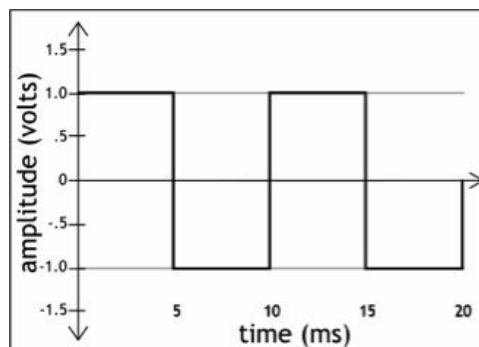


A RIMM (following) with its CRIMM (preceding)



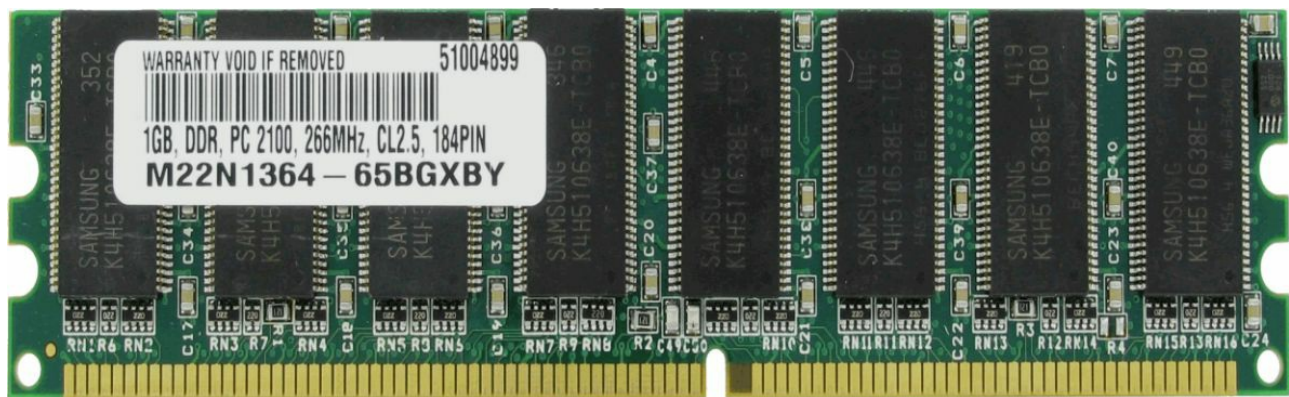
# Synchronous Dynamic RAM

This version of RAM was designed to be tied to the same clock speed as the processor. The square wave or binary tick of the crystal clock acts as a metronome to keep all components of the system in-step, and here the rising edge of the clock input is when any changes to the control inputs are noticed. Effectively, it could receive the next instruction as it's writing the last one, making this system more efficient than asynchronous RAM:



A square wave

By writing command instructions on both the rising and falling edges of the square wave, we can send double the commands we could otherwise:



1 GB DDR RAM at a clock speed of 266 MHz, 184 pin

Notice that, with DDR RAM in particular, we use the number of pins to determine the bandwidth, and to indicate the device the RAM stick is to be used in. Each stick's form factor contains connecting pins on the lower edge, with a notch at various points across the stick. These are used to guide the stick into position and to prevent the user from adding the wrong type of stick onto the motherboard slot. (A process referred to as **keying**.)

The number of chips on the stick is typically an even number. If there is an additional chip, the extra chip is used to create an **error correcting code** calculation, to run a rudimentary check that data being stored is consistent and does not contain an error:

### DDR standards and pins

DDR SDRAM standard	Release year	Bus Clock (MHz)	Transfer Rate (MT/s)	DIMM pins	SO-DIMM pins	MicroDIMM pins
DDR1	2000	100-200	200-400	184	200	172
DDR2	2003	200-533.33	400-1066.67	240	200	214
DDR3	2007	400-1066.67	800-2133.33	240	204	214
DDR4	2014	1066.67-2133.33	2133.33-4266.67	288	256	-



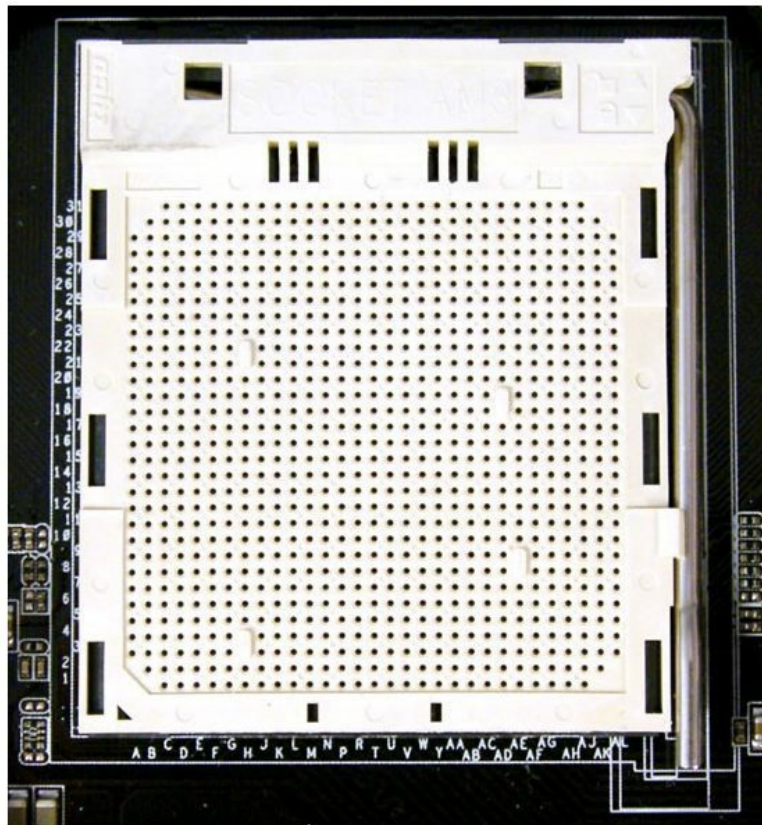


# CPU sockets

The processor, or **Central Processing Unit (CPU)**, forms the center of the system. Data and machine code is broken down into binary. The processor takes this binary stream of data and performs mathematical calculations, which then are sent to the appropriate hardware peripheral, or to memory, for use. The CPU is very much the brain of the system and a typical motherboard can support different types and speeds of processor, each having an amount of capacity and different calculation speeds. Two major companies, AMD and Intel, have designed similar processors, which have grown sequentially over time. For reasons of caching and circuitry design, Intel are the standard and their benchmarks produce speeds accurate to the speeds advertised for their processor. AMD is slightly cheaper, often does not contain the built-in caching and performance benefits, and does not clock to the exact figure quoted, but they are popular with the gaming community and work just as well in most test cases. Microsoft builds their software with Intel systems in mind, but accept that their systems will work with other processors where those processors are similar to Intel's processor.

The processor connects to the motherboard typically via a socket, a pin board in the shape of a square. The socket comes in two types--**lever** or **clamshell**, depending on the manufacturer. These accept an array of gold pins, each of which connects to data bus lanes. On 32-bit systems the processor pins feature around the outside of the base of the processor. On 64-bit systems there are considerably more pins and the entire base of the processor is taken up with an array of pins. The pin array is keyed, meaning that you will notice a notch, or missing pin, in one corner, which denotes **pin 1**. This corresponds with a missing hole on the socket array.

All socket processors require no force other than gravity to insert the processor into place. The entire array should drop into place. The clamshell lid is then closed over the processor, or with the lever the lever is lowered, locking the pins in place. Due to the fact that the processor produces, a considerable amount of heat a non-conductive gel (similar to tile grout) is applied to the top side of the processor and then a heatsink with fan is locked into place, clasping the processor and socket. No air gap is present between the processor and heatsink, otherwise a hotspot may be created, reducing the life of the processor. Air is blown through the heatsink fins, where it is heated and then exhausted through the back of the chassis:



An AM3 lever processor socket with keying notches

In terms of form factor, CPUs are either land-grid, or pin-grid arrays, with the notable exceptions of the Pentium II and III, which had their own plastic heatsink case, which was a slot system:



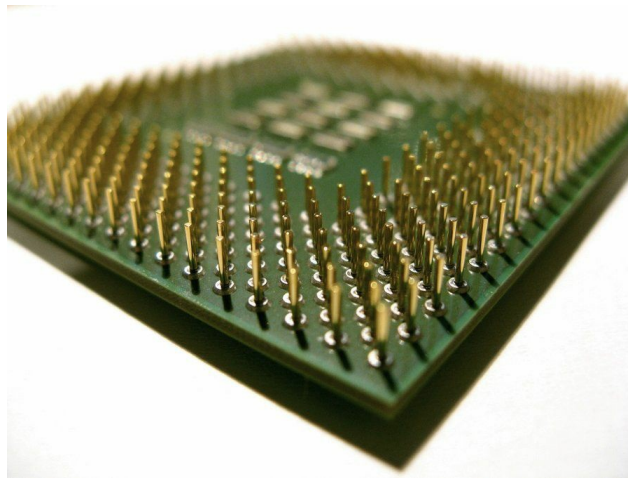
The Pentium II slot processor

Notice in contrast the Pentium 3 also was a slot-based processor, but heat problems led to a return to the socket processor.



The Pentium III slot processor

With both AMD and Intel returning to the socket the battle was still over which was more efficient--Pin-Based or Land-Based arrays:



Pin Grid Array on the base of the CPU

Here is a land-grid array. Notice the difference:



Land Grid Array on the base of the CPU



List of 80x86 sockets and slots  
Refer to Appendix A



# Chipsets

The motherboard, or mainboard, refers to the central circuit board, which serves as the **central nervous system** for the PC. The CPU and memory together form the brain and here all calculations are performed. This flow of data between the calculating component and the storage component is referred to as the **Northbridge**.



# Northbridge

The flow of data into and out of the Northbridge takes place along a data bus and is controlled by the Northbridge processor, which orders the packets of data and prioritizes them.

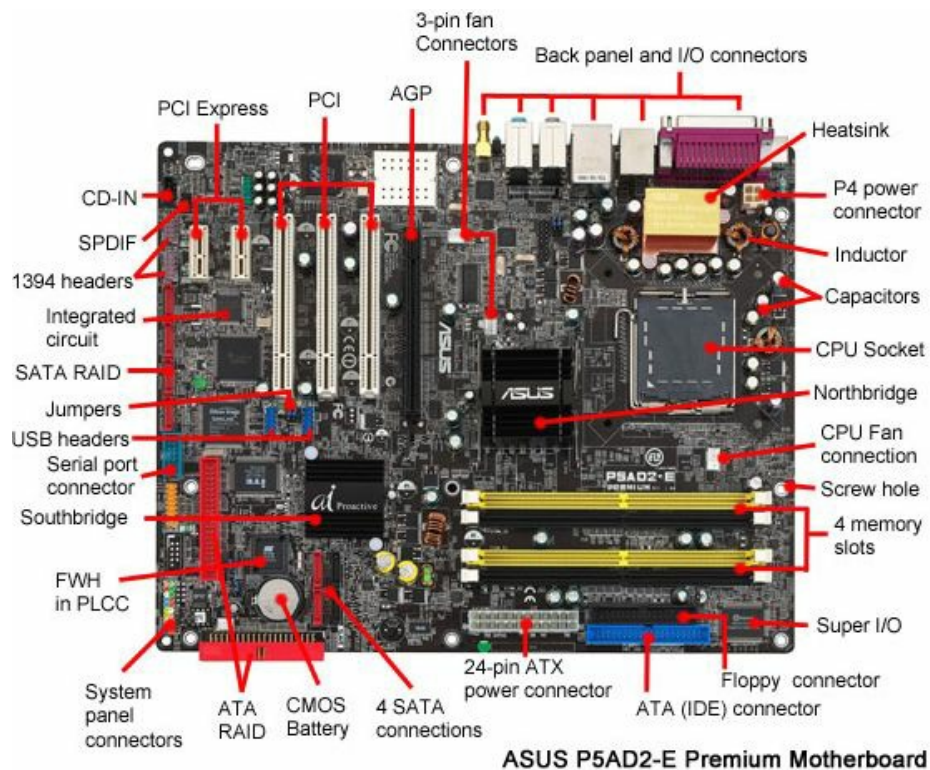




# Southbridge

The **Southbridge** is the southernmost portion of the circuit board onto which extension peripherals and expansion cards are fitted. The outside world communicates through the Southbridge and similarly, data is sent on a data bus and prioritized by using the Southbridge processor passing data into the Northbridge.

On the original IPM PC, the main circuit board located on the base of the PC had everything connected to it but only one expansion slot. This connected a daughter board, or riser card--a card extending the functionality by allowing further expansion slots and therefore also cards to connect to the bus. Cards were installed into the riser so that they sat stacked above each other. We have now integrated the riser/daughter with the mainboard, and the terms motherboard and mainboard are used interchangeably:



A labelled ASUS motherboard. Expansion slots are top left of the image



# CMOS battery

The lithium battery provides residual power to keep the clock running, ensuring that the BIOS saved settings are retained once the main power is off.



# Power connections and types

The motherboard is powered by Direct Current supplied by a step-down transformer, referred to as a **Power Supply Unit**. The power supply converts mains AC to lower voltage DC, typically 12, 5, and 3.3 volts in both directions. The main **rainbow** cable, known as P1, is typically 20 or 24 pin on the ATX system (the extra four pins are used to supply additional power for high-end processors and for integrated graphics card).

On some systems, the 4-pin block can attach to the 20-pin P1 block, whereas on others the 4-pin block is located further away from the P1 block. This 4-pin block contains two yellow and two black wires supplying the additional 12V, and is referred to as P2.

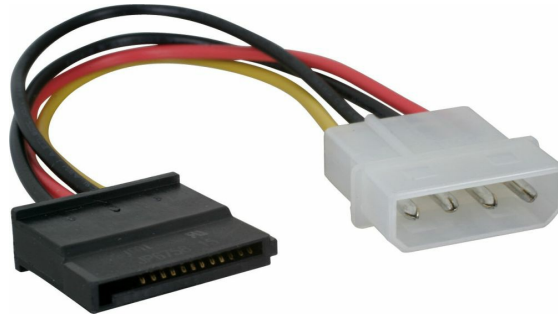
Internal peripherals are also powered by the power supply. The standard power connector is the Molex, offering 5 and 12-volt options:



A Molex connector supplying 5 and 12 volts



Mini Molex adapter



Molex to SATA converter

But how much power do I need to produce? Each component has a required wattage. If you add up the power consumption for the entire system, this will typically be between 300 and 900 Watts, dependent on the specification of the system. If you are unable to supply all of the required power then the system may not be able to completely function, so it is good practice to calculate the overall wattage consumption before building your system.



Remember, to calculate Power (Watts) we multiply the voltage (Volts) by the current (Amps):

$$W = VI$$





# Fan connectors

The mini-Molex (also referred to as a Berg connector) is used to connect to specific motherboard devices, typically to power chassis and heatsink fans or internal lighting. It used to be commonly used to power floppy disk drives.

**Serial ATA (SATA)** hard disk drives have a proprietary power connector and are now standard on most power supplies.

CPU fans and chassis fans are commonly powered by mini 4-pin connectors found on the motherboard, located near to the processor socket. Other additional chassis fans and lighting need to be powered from spare Molex plugs, from the power supply.

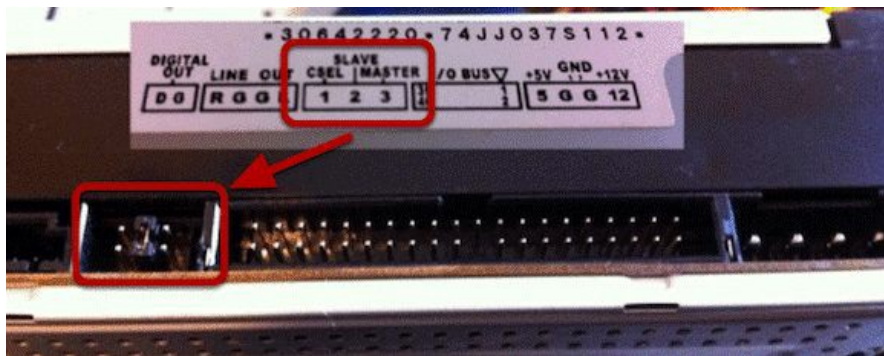


# Data connectors

The motherboard typically contains parallel data channels for IDE. There will be two IDE slots, which support a 40-pin data ribbon cable (the red stripe on the side of the ribbon denotes pin 1, otherwise the slot is keyed). The cable extends to two devices. To support both devices an identification signal is used to denote the device as either **master** or **slave**. This is set on the back of the drive. The **Cable Select** option is used with the more recent 80-wire (40 are used for shielding) Ultra DMA cables. Here, master is the device at the end of the cable. Standard IDE cables do not support Cable Select:



80-wire Ultra DMA cable



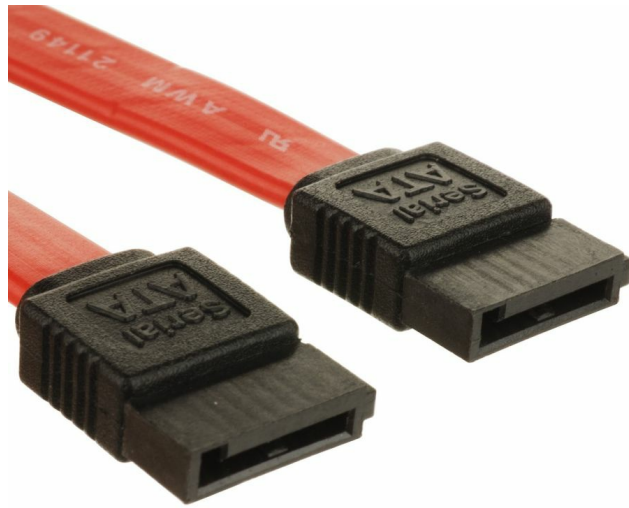
Master/Slave/CS selector, IDE data socket and Molex power socket on an IDE CD-ROM drive

Within the BIOS the data cables are scanned, and you will notice up to two recognized devices per channel (ribbon cable).

IDE is a derivation of the SCSI standard, which was used to support up to 16 drives on one cable. Each needed to have a unique ID number set on the switch at the back of the drive, and a terminator block was added to the last drive to complete the circuit.

IDE is being phased out. We now use a serial connection system with dedicated sockets

per device--SATA. With SATA, the cables are shorter and inexpensive, drives are hot-swappable, data is transferred at a greatly increased rate, and transfer is more efficient as a new I/O queuing protocol is used:



Serial ATA connectors

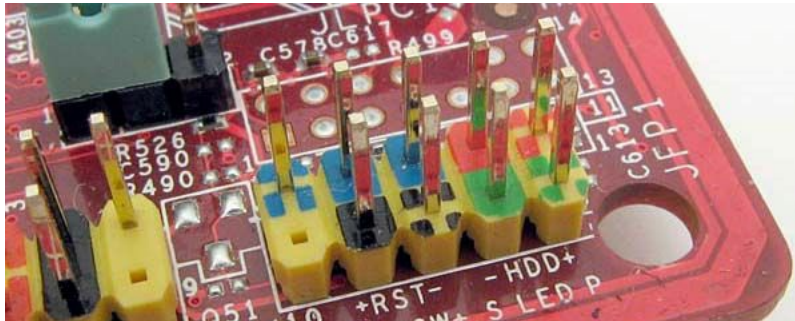
With SATA, notice that the data cable is quite thick and sturdy, but surprisingly small in comparison to IDE, containing seven pins. The SATA power plug is quite wide, but in reality only a few wires are actually used to power the device out of the 15 pins available.



# Front/top panel connectors

The **header** is a set of pins in the east corner of the motherboard, which connect to LEDs and switches located at the front of the PC chassis.

Nicknamed **the umbilical**, this set of wires connects the drive response light, power LED, reset switch, and main power switch:



Front panel connectors



Panel wire connectors

It is worth noting that modern PCs, since the mid-1990s, are **soft power** devices. Up to that point there was a high-duty power switch on the front of the chassis, which was connected to and supplied power to the power supply. From the ATX motherboard onwards, the motherboard is constantly receiving some power from the power supply but is in a sleep state. The power switch closes a circuit on the motherboard to send a signal to wake up the board, at which point full power requirements are met to load the system. This signal is under software control, so the system's power state can be altered by a **Magic Packet** (Wake On LAN) or by the OS (for example, `shutdown` command, or Turn Off GUI button in Windows).





An early chassis face with power button

The motherboard also contains pin headers for USB cables. The USB cable is typically keyed and 5-pins, so is easy to fit onto the header. Most motherboards now support four USB headers.

Audio can also be extended to the front panel--3.5 mm jacks for audio in, mic-in, and audio out (for headphones) can connect directly to the integrated sound card on the motherboard:



Front panel audio and USB ports



USB plate and header cable





# Bus speeds

With early pre-Pentium systems, it was common to see a Turbo button, which would double the bus speed. This is now set within the BIOS, but should not be changed as the bus speed is measured by the OS during install and is checked upon loading. The system may become unstable if the bus speed is altered after the OS has been installed.

As previously mentioned, the Front side bus is the heartbeat of the computer. It is the speed at which the RAM and processor use and stay in synchronization. The back-side bus could be the same but is often a different speed, but is a multiple of the front-side bus. Data can therefore be sent faster than is needed by the processor and queued in the buffer cache. HyperTransport, Intel QuickPath Interconnect, or Direct Media Interface are now used to replace the older concept of front and back-side buses, and are typically used on Intel processors and supporting hardware.



**Exam tip:** Expect to have to calculate the processor speed using the FSB frequency and the number of transfers per cycle as follows: A 64-bit (8-byte) wide FSB operating at a frequency of 100 MHz that performs four transfers per cycle has a bandwidth of 3,200 megabytes per second (MB/s):

$$8 \text{ bytes/transfer} \times 100 \text{ MHz} \times 4 \text{ transfers/cycle} = 3200 \text{ MB/s}$$



# Reset button

The reset button clears the RAM and forces the PC to restart from the **Power On Self Test (POST)**. Once it has passed POST, the BIOS configuration is loaded, then the OS will start to load (the process of loading the OS is referred to as **bootstrapping**).

Exam tips:



Memorize the parts of the motherboard. Label a diagram of your own motherboard, if you have access to it.

Attempt a few processor speed questions and understand that you have to express the answer in mb/s, hence the need to transfer by 8 (there are eight bits in one byte).

Think about different scenarios where build will differ. For example, an architect may need a high-end system with large graphics capabilities. A file server will need multiple large disks, both internal and external.

The term e-SATA only means external SATA, to distinguish an external hard drive from an internal hard drive.



**How to build your own PC--online guide:** <http://buildapc.nzxt.com/>

**Motherboard parts quiz:** <http://www.imagequiz.co.uk/quizzes/2149007>



# Video training

To summarize this section I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **An Overview of Motherboard Types (8:31):** <http://www.professormesser.com/?p=19309>
- **Motherboard Expansion Slots and Bus Speeds (12:48):** <http://www.professormesser.com/?p=19325>
- **Motherboard RAM Slots (4:17):** <http://www.professormesser.com/?p=19329>
- **CPU Sockets (3:24):** <http://www.professormesser.com/?p=19335>
- **Motherboard Chipsets (6:43):** <http://www.professormesser.com/?p=19339>
- **Motherboard Jumpers and Connectors (4:25):** <http://www.professormesser.com/?p=19342>



## 901.1.3 Compare and contrast various RAM types and their features

RAM is a storage area in which data currently in use is stored. Data is stored in blocks, each with an ID number attached to it referred to as an address. Unlike the mechanical IDE drive, or tape drive where you have to move the actuator arm to the correct position, or with the tape, the tape is spun to the correct point in which we can record. Here there is a degree of latency while the correct position is found. In RAM, however, each block is immediately accessible. This is also the case with solid-state drives, which also access at the same time with no residual latency.

There are two types of RAM--static RAM is extremely expensive, and here a series of physical switches are set and changed repeatedly. If the power were to be switched off, the switch states are retained, so no data is lost. However, this is not practical for the home market. Conversely, dynamic RAM requires a constant supply of power to retain the data in memory. The RAM chip also needs to be refreshed repeatedly and constantly every few seconds, so in that respect data is not as reliable, and could be corrupted or lost. If the power were to be switched off, all data in RAM will be lost.

Data in RAM comprises of actual session data the user is working on, as well as session data concerning the OS and driver data allowing the machine to communicate with the hardware. For example, I am currently typing this book using a Word Processing application, on a Windows 10 system, on my laptop. If I did not save the document and powered off the laptop all of my work would be lost and the system would have to restart.

In section 901.1.2 we covered RAM types from a physical perspective but also looked at signaling, referring to the single and double data rate. Here we will cover RAM types and their compatibility.





# Types

In this section, we will look at an array of RAM types and how they have progressed over the year. For the exam, have a good understanding as to which RAM types are used with which processor and, therefore, on which type of motherboard.

RAM is keyed, so it is not possible to install a RAM chip into the wrong RAM slot, but the frequency at which the RAM runs is set in the BIOS. We will therefore also look at some of the differences in the type of RAM available as well as just the physical pin count.



# DDR

**Double data rate synchronous dynamic random-access memory (DDR SDRAM)** has now been superseded. However, it is a valuable lesson to learn our starting point in terms of RAM data transfer speed and to look at how this is reliant on the Memory bus's clock rate, whether the data is single or double data rate. If the data is transferred in blocks of 64 bits, so a DDR stick with the model of DDR-200 gives a transfer rate of  $(\text{memory bus clock rate}) \times 2$  (for dual rate)  $\times 64$  (number of bits transferred) / 8 (number of bits/byte). If the frequency therefore is 100 MHz, DDR SDRAM would provide a maximum transfer rate of 1600 MB/s.



# DDR2

DDR2 replaced the original DDR and ran to 2007, when it too was superseded. The data was double-pumped, meaning that two blocks of data were sent on both the rising and falling edges of the clock signal. As this is the case, the benefit of DDR2 was clear -DDR2 memory sticks are at least twice as fast as DDR.

In the example of the DDR2-400C stick, with a frequency of 100 MHz, the rate is double-pumped, so the rate is now 4, instead of the earlier two. The example if a DDR2 stick were to be used would be as follows:

$100 \text{ MHz} \times 2 \text{ (double pump)} \times 2 \text{ (dual rate DDR)} \times 64 \text{ bits/8 (bits/byte conversion)} = 3200\text{MB/s}$



# DDR3

**Double data rate type three SDRAM (DDR3 SDRAM)** was launched in 2007 and has now been superseded by DDR4. It supports ram sticks of up to 8 GB, and this time the data is quadruple-pumped, so:

$100 \text{ MHz} \times 4 \text{ (quad pump)} \times 2 \text{ (dual rate DDR)} \times 64 \text{ bits/8 (bits/byte conversion)} = 6400 \text{ MB/s}$

With four ranks of 64 bits, one DDR3 stick can actually support 16 GB.





# SODIMM

The laptop equivalents had a smaller form factor. SODIMM is in fact approximately two thirds the size of its PC equivalent. Typically, there are two RAM slots in a laptop, either side of the motherboard. One is located on the rear and is accessed by removing a back plate, the other requires you to remove the keyboard to access the slot.



**Exam tip:** Revise the pins! You will find these on Obj 901.1.2.



# DIMM

**Dual inline memory module (DIMM)** refers to the fact that there are two ranks of chips, one either side of the circuit board (stick). Whereas DDR and SDRAM refer to how the stick functions, DIMM refers to the physical layout of the chips on either side of the stick. This is in contrast to the earlier SIMM module, where the chips were printed onto one side of the circuit board.



# Parity versus non-parity

In parity-supported sticks, an additional chip is in use in the rank (so you will count nine, not eight, chips on the stick). The additional chip stores a parity bit (a checksum) created from the byte of data being stored to the RAM stick. The parity bit is either even or odd. As a basic concept, imagine that the byte of data being stored is put through an error-checking process, which calculates a checksum number (for example, 65535). As you can see, this number ends in 5, which is an odd number, so the parity bit should be 1 if the rule was to only store a parity bit if the calculated number is odd. This is not a very good error-checking technique, but can be calculated quickly as each byte is stored.



# ECC versus non-ECC

**Error Correcting Code (ECC)** is more expensive, as further calculations take place to ensure the integrity of the byte being stored. With ECC, the byte is analyzed, and if an error is found the data is resaved, hence **error correcting**. This can slow the system a little but is useful when you need to rely on data being stored as absolutely accurate. It is up to the OS to flag that there may be an error in the data, at which point the data in memory can be corrected without any impact to the application, which is running in memory.

Most RAM you will encounter, certainly for home use, is non-ECC. It is prone to error occasionally, but is cheaper.





# RAM configurations

As we discussed in obj 901.1.2, the color pairs on the motherboard's RAM slots shows that the RAM is a dual-channel set. You should install two matching RAM sticks into the same color pair to get the advantage of dual channel. If you decide to add two more sticks, these should match the speed and capacity of the first two, otherwise the motherboard will "downclock" the four sticks to all work at the slower speed.



# Single channel versus dual channel versus triple channel

As indicated above and in obj 901.1.2, some RAM sticks are not independent. For example, on a dual-channel system 2 x 4 GB sticks provide 8 GB of available memory, but we can write out 4 GB at the same time, to each stick. Triple channel extends the analogy further--here, the memory bus is expanded to 192 bits by using three memory modules at the same time. This is only available on the Intel Core i7 processor motherboards with socket LGA1366:

- **Single sided versus double sided:** Although single-sided RAM may have chips on both side of the circuit board, each side is independent, whereas with double-sided RAM, all of the chips on the stick operate as one group.
- **Buffered versus unbuffered:** With buffered RAM there is a separate cache between the motherboard data controller and the RAM stick, ensuring that the data flow is smooth and constant. Buffered and unbuffered RAM are keyed differently to avoid the wrong type being used.
- **RAM compatibility:** With most of these examples all RAM is keyed and is not backward compatible.
- **\* Timeline:**
  - **Single Data Rate (SDR)** technology primarily appeared in systems manufactured before 2002
  - **Double Data Rate (DDR)** technology began to appear in systems manufactured in 2002
  - **Second Generation Double Data Rate (DDR2)** technology began to appear mid-2004
  - DDR3 technology began to appear in late 2007
  - DDR4 technology began to appear in 2014



# Exam questions

1. How many pins does a DDR1 desktop memory module have?
  1. 184
  2. 168
  3. 200
  4. 240
2. How many pins do DDR2 and DDR3 memory modules have?
  1. 72
  2. 240
  3. 144
  4. 184
3. How many pins does a RAMBUS or RIMM memory module have?
  1. 240
  2. 72
  3. 168
  4. 184
4. What does ECC stand for?
  1. Error Correcting Code
  2. Edit Correcting Chip
  3. Erasable Correcting Code
  4. Equal Correcting Communication
5. Laptop memory modules come in which sizes?
  1. 72
  2. 144
  3. 200
  4. 204
  5. 68
  6. 168
6. A DDR memory module has a Clock Speed of 100 MHz. What is the PC Speed rating?
  1. PC800
  2. PC1600
  3. PC2400
  4. PC4800
7. A DDR2 memory module has a DDR2 Speed Rating of DDR2-1000. What is the Core RAM Clock Speed?

1. 250
  2. 500
  3. 800
  4. 8000
8. A DD3 memory module has a DDR I/O Speed of 800 MHz. What is the PC Speed rating?
1. PC3-12800
  2. PC3-6400
  3. PC3-17000
  4. PC3-10667
9. Do DDR2 memory modules fit into DD3 memory slots?
1. Yes
  2. No
10. CRIMMs are used with what technology?
1. DDR to add speed to the RAM
  2. RDRAM to terminate
  3. Synching the RDRAM to the CPU
  4. To enable quadruple channel memory
11. What does DIMM stand for?
1. Dynamic Inline Memory Module?
  2. Data Inline Memory Module
  3. Dull Inline Memory Module
  4. Dual Inline Memory Module



# Video training

To summarize this section I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **An Overview of PC Memory Types** : <http://www.professormesser.com/?p=19342>
- **Understanding PC Memory**: <http://www.professormesser.com/?p=19360>





# 901.1.4 Install and configure PC expansion cards

A motherboard is limited as to what it can do and on-board components such as Network capabilities, or the quality of the sound card may be improved by using a dedicated card. These need to be fitted into the internal slots and the on-board functionality disabled. This section describes all of the various additional cards you can install to expand the functionality of your system.

Always ensure that you follow the correct health and safety procedures when installing any component. Unplug all power to the system before attempting to work on it. Remove the chassis to a workbench and use anti-static protection equipment. This will ensure that static electricity built up on your skin is not transferred to the components.

If you do shock a chip, for example, RAM, you will not notice the damage straight away. In fact, it may take months before errors start to turn up, but the equipment is extremely delicate and sensitive.

Use a toolkit with a screw pot and ensure to make notes as to where everything needs to go, if you are dismantling the system. One key port to make note of is the USB devices, as the drivers are tied to the port you have plugged the device into. If you refit the USB device to the wrong port the device will be recognized as a new device and re-installed as a new object in the OS.

All PCI components are fitted to the chassis as follows:

1. Identify the blanking plate currently covering where your new card is going to reside. Remove the blanking plate by pushing at the corners, loosening the perforated metal. Wiggle the plate until it becomes loose and can be removed by hand.



**Warning!** The bare metal is sharp and may cut the skin. Please be very careful.

2. Line up the gold connector pins over the PCI slot. Place the metal tab at the base of the card on its face against the back of the chassis. Ensure that the gold connector

pins are still in line. Apply equal pressure downwards, pushing the pins into their grip contacts.

3. Add a screw to the locking clip at the top of the face plate. This screws into pre-drilled holes by the blanking plates.

Only take out blanking plates that you need. As the chassis contains fans, the inside of the PC is slightly pressurized. The aim is to suck in cold air from the front of the PC and expel the hot air from the exhaust holes in the rear. If other gaps are present in the rear of the chassis then the air simply will not flow. Also, there is a greater chance of dust or other foreign objects entering the PC. Over time, this dirt will accumulate and stop the fans, leading to heat issues and burnout.



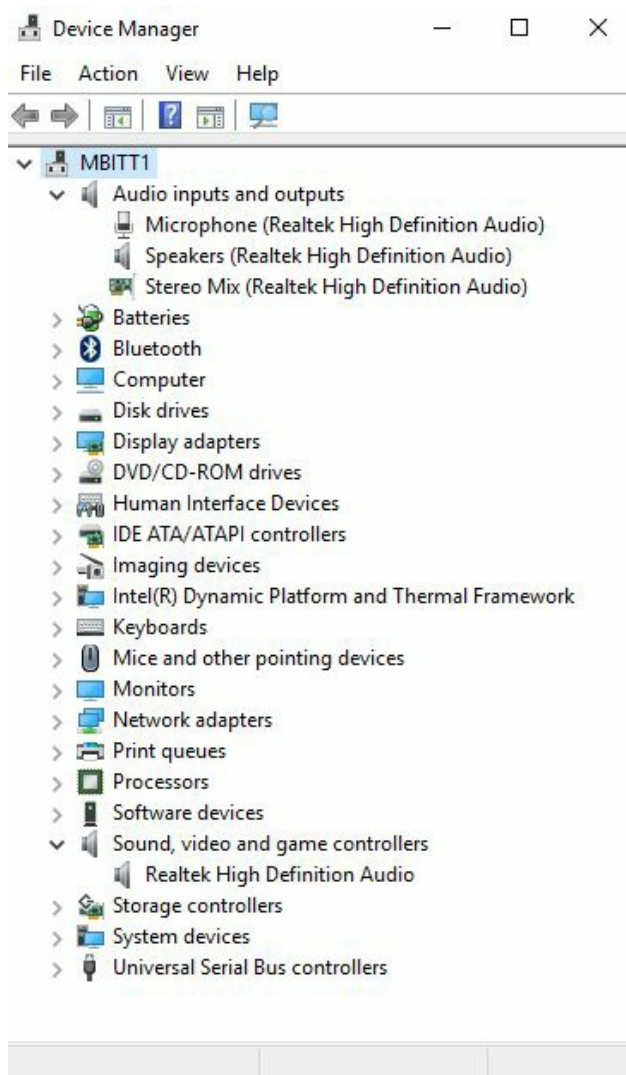
# Sound cards



For a detailed how to guide visit this link: <http://www.wikihow.com/Install-a-Sound-Card>

Once the card has been physically installed, reconnect your PC and boot it up. If you go to Device Manager you will notice that either a generic Microsoft-supplied driver is used or the device may be unknown. It is advisable to load the drivers by running the installation file found either on the accompanying disk, or by downloading the driver relating to the model of sound card from the manufacturer's website.

Once the driver has been loaded, Device Manager should recognize the device. The entry for the object will be renamed, started, and placed into the Audio category:





NB: When you are installing printers and scanners connected via USB it is important to install the driver first. The installation wizard will prompt you to discover the physical print device later on in the installation.

Most modern integrated motherboards have built-in audio capabilities, so there is only a need for a separate audio card if you require additional functions, for example, for home cinema theater systems to support Dolby, or 5:1 channels.

You will also notice that the CD supplied with the audio card will contain supporting software to enhance the experience (for example, it may contain a multi-track editor):



A sound card



# Video cards



For a detailed how to guide visit this link: <http://www.wikihow.com/Install-a-Graphics-Card>

Most modern motherboards contain a basic video card with a small amount of RAM. In early systems, the graphics card's RAM requirements were met by using the existing RAM available to us. A portion of available RAM would be reserved specifically for use by the video card. This is known as shared RAM.

Gaming PCs in particular have very large graphics processing requirements, so separate dedicated graphics processors are installed onto the graphics card. These are very powerful and require their own power cable, so you have to ensure that your power supply can provide the wattage needed.

Moving from one manufacturer's video card to another is not an easy task. The two main providers at the time of writing are NVidia and ATI Technologies. The software used by these providers is only compatible with cards produced by the manufacturer, so if you are swapping from ATI to NVidia (for example), the best solution is to uninstall the graphics card and revert to a basic VGA driver supplied by Windows (it will automatically find a compatible graphics driver, so you have to ensure that we are using the basic before we can continue). This removes files and registry entries from the old software. Next, physically swap over the video cards, install the new one, then boot into the OS using the new card. It will detect the new card, but again ensure that you choose the basic driver, as further registry changes are needed to remove references to the old one. Then reboot and install the new graphics card's software. Reboot a further time to use the video card at its full ability:





Graphics card



# Network cards

The NIC allows for communication across the network to other computers and devices (for example, printers). The NIC is typically integrated onto the motherboard, although you can purchase faster NICs as separate cards, which are wireless, or use fiber-optic cable instead of standard Ethernet copper cable.

The NIC can be shared with any virtualized PCs hosted by the computer through the virtual switch. The virtualized PCs each have their own NIC, emulating the role of an actual NIC. The virtualized NICs can exist on the same subnet as physical devices allowing virtualized PCs. The only limitation is, by sharing the bandwidth used by the actual NIC, the data transfers for each device are queued through the physical NIC, which will also have its own data to send.

The NIC is the physical component connecting the PC to the network. It meets layer 1 (physical layer) of the **Open Systems Interconnect (OSI)** model in that we are physically attaching the computer to the network and sending a signal. It also meets layer 2 of the OSI model in that a data frame is sent, using a specific number (written in hexadecimal) to define where the frame should be sent to, and also a Hex number to show where it has come from.

A NIC requires the following information to be able to communicate.



# Protocols and services

- **TCP/IP protocol stack:** We typically use IPv4 on the local network, although we can also use IP version 6. An IP address is a unique number assigned to a computer so that it may be found on the network. It identifies the PC to any other PC. Using a more human analogy, consider this as similar to your mobile phone number. The **Transport Connection Protocol (TCP)** checks the quality of the data packet being sent and ensures that the packet is error-free. The IP protocol is concerned with where to send the data and where it has come from. TCP operates on layer 4 of the OSI model and IP operates on layer 3.
- **Client for Microsoft networks:** This is effectively the login page. It is required to allow authentication across the network.
- **QoS packet scheduler:** This is used to prioritize video and audio traffic over a network connection, ensuring that a video conference (for example) continues to be live and not interrupted, as the PC may use the NIC for other traffic as well.
- **File and printer sharing:** Without this, network shares and network printers would not be accessible.

The NIC requires the following to be configured:

- **IP address:** This is a number written as 4 x 8-bit parts. The numbers therefore range from 0.0.0.0 to 255.255.255.255. IP addresses are considered to be either **public** (that is, you have purchased the number for use and it is accessible globally), or **private** (for internal use).
- **Subnet mask:** This is used to split the IP address into two different pieces of information:
  - Which subnet you are on (which part of the network)
  - Your PC number (your host number) on that network portion
- To find other computers on the network, the client PC needs to know where to find the DNS server. The DNS server is responsible for keeping a phone book of IP addresses. If you want to communicate with another computer, typically you would navigate to that computer by its computer name, but DNS allows your OS to use its IP address.
- **Router gateway:** The router is a device that connects two or more subnets (network sections) together. It can be considered as a doorway allowing traffic out of the subnet and onto the wider network, or onto the internet:



Network Interface Card (NIC)



# USB cards

A USB card provides additional USB ports, allowing you to connect more devices at the same time. These typically contain a controller card and operate as a USB switch, allowing several port connections using the same USB header:

- USB supports up to 127 devices on one cable
- USB 1 supports speeds up to 1.5 Mb/s but has a full speed of 12 Mb/s
- USB 2 typically transfers at 280 Mb/s but has a full speed of 480 Mb/s
- USB 3 typically transfers at 4 Gb/s but has a full speed of 5 Gb/s

USB 3.1 is also planned, with speeds of up to 10 Gb/s, and is backward compatible with both USB 2 and 3:



USB expansion card





# FireWire cards

As with USB, FireWire cards allow communication using the Firewire cable. This was developed by Apple in the early 1990s and is the Apple equivalent of USB. It has been standardized as IEEE 1394. This is a very fast technology often used with media devices, cameras, and analog to digital converters where the flow of data into the PC has to be very fast. FireWire supports up to 63 devices on one cable:

- FireWire 400 (IEEE 1394-1995) can transmit at 100, 200, or 400 Mbit/s half-duplex
- FireWire 800 (IEEE 1394b-2002) supports data rates up to 3200 Mbit/s (400 MB/s)

Sadly, FireWire was considered obsolete in 2008, although is now relaunched as a public domain item in 2017.

One advantage over USB was the fact that the speed was instant, whereas the quoted speeds for USB are achieved in stages as the data transfer gets ever faster, eventually leaching the limit:



FireWire card



# Thunderbolt cards

Developed by Apple and Intel, the Thunderbolt is commonly found on Mac systems such as the MacBook air. It was first launched in 2011 and uses a mini Displayport connection. Modern equivalents now use a USB type C port.

Thunderbolt can transmit PCI Express and Displayport data, as well as providing DC power, which makes it ideal to attach to recording devices such as digital movie cameras. Thunderbolt C can transmit at 40 Gbit/s (5 GB/s), surpassing FireWire:



Thunderbolt card



# Storage cards - memory cards

Other storage options are available and are typically used to store data onto SIM cards or video camera cards. Data sizes vary. Notable formats are as follows:

- **Secure Digital card (SD)**
- MiniSD Card with an SD card adapter
- **CompactFlash (CF-I)**
- Memory Stick
- **MultiMediaCard (MMC)**
- SmartMedia
- xD-Picture Card

Name	Abbreviation	Form factor
PC Card	PCMCIA	$85.6 \times 54 \times 3.3$ mm
SmartMedia	SM/SMC	$45 \times 37 \times 0.76$ mm
Memory Stick	MS	$50.0 \times 21.5 \times 2.8$ mm
Multimedia Card	MMC	$32 \times 24 \times 1.5$ mm
Secure Digital card	SD	$32 \times 24 \times 2.1$ mm
miniSD card	miniSD	$21.5 \times 20 \times 1.4$ mm
xD-Picture Card	xD	$20 \times 25 \times 1.7$ mm
XQD card	XQD	$38.5 \times 29.8 \times 3.8$ mm



A typical SDcard





# Modem cards

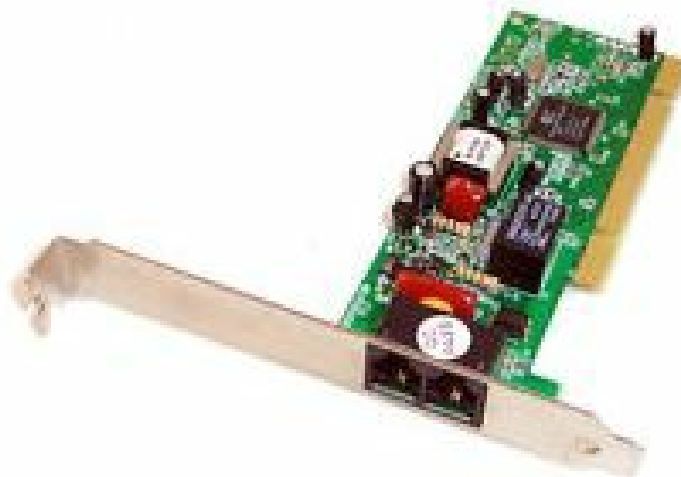
The Modulator/Demodulator card allows for data transmission and connection to a network over a phone line by sending binary data as audible sounds along the carrier wave. The modem connects the PC to a phone line using an RJ11 port. Most modems also allow a phone to plug into the card to be used to monitor the line, but can also allow you to make normal phone calls when the line is not in use.

This technology is by today's standards extremely slow and unreliable, with a typical v90 modem connecting at 56Kb/s, but in reality only achieving speeds of approx. 32-44Kb/s.

These were very much the first technology used to connect a remote PC to a network, and without this card the internet might never have had the success it has had. Early modems were separate peripherals that connected to the PC through the parallel (although some used the COM2 serial) port, but it is more common to find v90 modems as an internal PCI card:



Visit the following URL to hear a modem connect a PC to the internet: <https://www.youtube.com/watch?v=vvr9AMWEU-c>



Modem card



# Wireless/cellular cards

As a variant to the NIC, wireless connectivity can be obtained through the addition of a PCI wireless card. The wireless card transmits on the 802.11 standard using either protocol a, b, g, or n (depending on speed and the protocol the router is expecting to receive). It is worth noting that, once the card has been installed, the antenna screws onto the antenna base on the side of the card:



A wireless adapter card



# TV tuner cards

The TV tuner card allows for the receipt of a UHF analog signal and from this the PC can be used as a standard TV. TV tuner cards are now considered to be obsolete as the analog signal is no longer being transmitted across the US, UK and other countries - TV transmissions are now digital:



TV tuner card



# Video capture cards

The video capture card is, in fact, an analog to digital converter. It is used to record a video signal in real time, which is then encoded and stored as a movie file. Video capture cards are processor-aggressive but were popular in the mid-1990s as stored video was digitized:



A video capture card

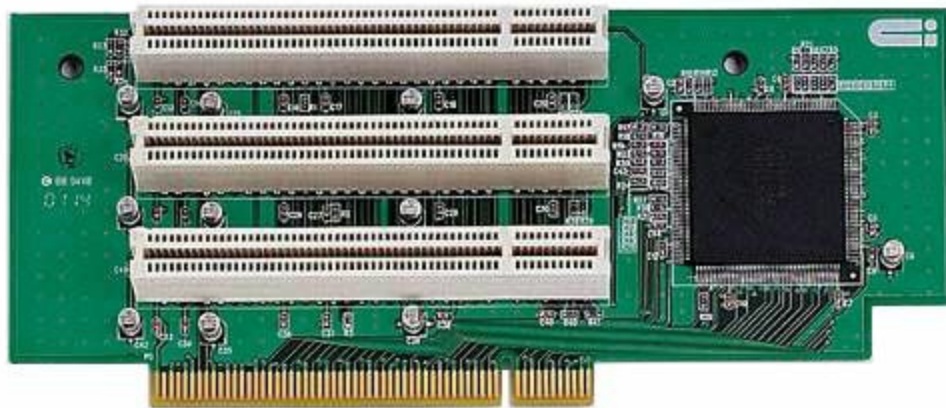




# Riser cards

The riser card is used to allow expansion cards to sit above the motherboard and were typically used on early IBM PCs. With modern motherboard design the expansion slots are integrated into the southern section of the motherboard and enable the cards to protrude at right angles to the motherboard.

Riser cards are synonymous with expansion cards and daughter boards. Where the expansion slots and control bus resides on a separate card, this is referred to as a daughter board (where the main Northbridge is the motherboard). Now, we use the terms mainboard and motherboard interchangeably:



A riser card



**Exam tip:** You will not be asked to identify the cards by sight, but rather explain what they are used for in the context of a scenario. For example: "Question: Simon is working away and wants to watch a TV show being aired on a terrestrial TV channel. What type of card does his PC need to have installed? Answer: TV tuner card."



# Video training

To summarize this section I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Installing and Configuring Expansion Cards (8:10):** <http://www.professormesser.com/free-a-plus-training/220-901/installing-and-configuring-expansion-cards-2/>



# **901.1.5 Install and configure storage devices and use appropriate media**

This section's focus is on storage--we will look at how we can retrieve data from a variety of different storage media, starting with optical storage technologies. The next part considers mechanical, magnetic hard disk drives and how they function. For the exam, note the different hard disk speeds available to you. We will consider how disk drives can be stored in an enclosure and called into use when needed (hot spares) and the fact that ATA drives can be replaced without having to turn off the system. Next, we will look at small, solid-state media used in digital cameras and smartphones alike.

We then detour to consider how the volume is formed and how, with RAID, we can either increase volume performance (read/write access speeds improved) or provide fault tolerance--the volume is still available if a disk fails.

We then consider backup media and mention the tape drive. The A+ exam does not now expect you to learn all of the different types of tape drive available as there has been a move to use external hard drives for backup over tape, which is much slower. Finally, we contrast the storage media's data capacity, comparing maximum storage values for each media.



# Optical drives

An optical drive is capable of creating pits in the reflective surface of a disk by using a laser to strike the surface of the disk. The pits and lands represent the binary 1 and 0 and can be read back by shining a lower-power laser light and determining if the receiver received the reflected beam, or if the beam is bounced off, at which point the reflector does not see a reflected beam.

A CD-ROM is a circular plastic disk with micro-pits etched onto the mirrored underside of the disk, which are created and read by a laser beam on an actuator arm. The laser can move from the center to the outside surface of the disk. The disk spins at 200-530 revolutions per minute (for x1 speed) and up to 1600-4240 rpm for x8 to x12 speed transfers.



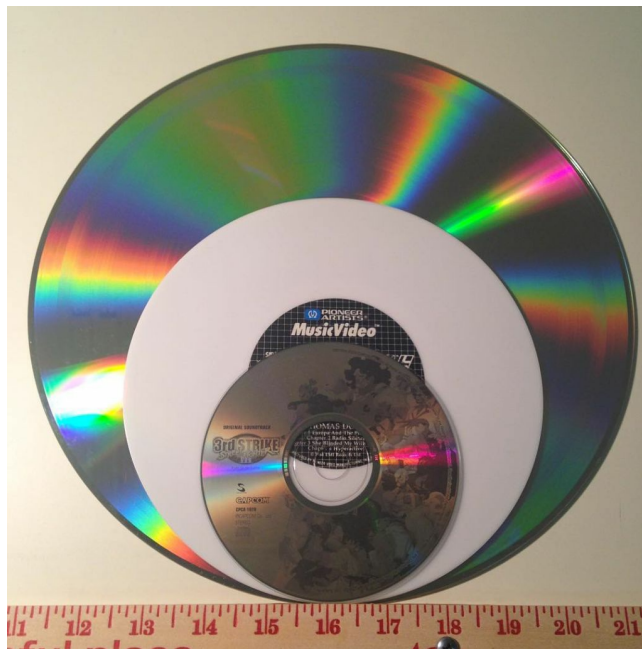


# CD-ROM/CD-RW

The CD is commonly associated with music albums. It is light and portable, but any scratches on the underside of the disk may cause the disk to jump and cause readability problems. The typical life of a disk is approximately five years, given for the fact that the greatest threat to a disk is humidity, causing the mirrored surface to peel away from the plastic disk.

CDs can be constantly rewritten to. These are referred to as rewritable, or CD-RW. Where data is stored in a read-only form we refer to it as a CD-ROM. The CD can typically hold 700 MB. CD-ROM disks are commonly associated with installation disks and can be used to store data. The most common format is actually the CD-RW, which can be purchased in packs or spindles. Due to their propensity and versatility they are cheap and easy to purchase.

Over the years there have been many variants of the CD. One notable version used for the domestic film and video market in the 1980s was Laserdisc--a now defunct format designed to replace the VHS recorder:



A comparison of the 12" common laserdisc, a rare 8" laserdisc used for shorts or film trailers and the standard 4 3/4" music CD



# **DVD-ROM/DVD-RW/DVD-RW DL**

The DVD format has a more concentrated format, with pits taking up less space. The DVD is identical to the CD in its physical structure and size, but can hold 4.7 GB per side. It is commonly used for gaming, or for installation media. As with CD, DVD's are rewritable.



# DVD-RW DL

Double Layer uses two recordable dyes, therefore allowing two sets of data to be recorded on the same surface. By doing this we are able to double the amount of data that can be stored on one side of the disk to 8.5 GB.



# Blu-ray

Now common for home use, Blu-ray offers high-definition video due to the amount of data that can be stored. A typical Blu-ray disc can store 25 GB single layer and 50 GB dual layer. It is common to purchase films in Blu-ray format:



The reverse side of a Blu-ray disc





# BD-R

A recordable Blu-ray disc is referred to as BD-R. It uses the Universal Disk Format, which is an open standard (ISO/IEC 13346). It is supported by a large number of manufacturers as a common format. Blu-ray uses UDF 2.5, which has metadata (keywords and author information about the media file) stored in a separate partition to the data.

Version 1 BD-R supports UDF 2.5 and AACS. The **Advanced Access Content System (AACS)** stores information for digital rights management (used in copy protection). AACS uses a decryption key to be able to read and decode the data on the player.

Version 2 was launched in 2006. It is backward compatible with v1 and features support for camcorders with the use of 8 cm disks. It supports the Blu-ray Disc Movie application format.

Version 3 was launched in 2010. The disk is multi-layered and uses the Blu-ray Audio Visual application format. It can store up to 100 GB and uses UDF 2.5 as the file system.



# BD-RE

BD-RE refers to the rewritable Blu-ray format.

Writing at 4.5 megabytes per second, version 1 was released in 2002, but is not compatible for use with PCs. It has a proprietary file system referred to as BDFS and uses the Blu-ray Audio Visual Application format (to decode the media on the Blu-ray player). It also supports content protection (BD-CP).

Version 2, launched in 2005, is computer-compatible. It supports AAC-ES.

Version 3 was launched in 2006. Similar to BD-R v2.

Version 4 was launched in 2010 and is similar to BD-R version 3.



**Power Tip!** Use markers that are Safe! Many markers have a chemical that eats the top layer.



# Magnetic hard disk drives

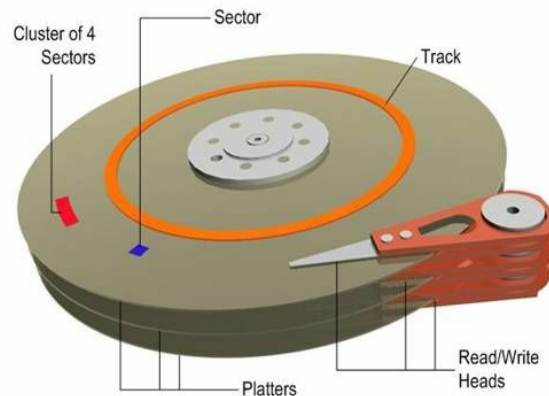
The magnetic hard disk drive is a metal disk coated with carbon metal oxide. An actuator arm with an electromagnetic head is used to magnetize sections of the disk surface, thereby reading and writing data onto the disk. Each disk has an actuator, and one spindle can house several platters.

The disks operate at different speeds and the speed is unique to the disk. Collectively, they are used to store data, and one drive is represented as one drive object within the operating system even though one drive contains multiple platters and surfaces.

Standard disk speeds are as follows:

- 5,400 rpm
- 7,200 rpm
- 10,000 rpm

The disk's surface area is split into blocks made up of sectors and segments:



Internal design of a Hard Disk Drive

In addition to this diagram, a cylinder refers to a selection of sectors at the same physical position but on every side of the spindle, making up a group (as if you were to drill a hole through them all at the position of the sector). Also, a block is an alternative name of one sector on one side. Programs such as CHKDSK and Defragger refer to blocks. A block is defined by its data size, not its physical area. Blocks on the outer section of the disk are therefore smaller than blocks nearer to the center. The surface area is equal, irrespective of position from the center.





# Hot swappable drives

Where a disk is replaced by the OS, or manually, is already powered up and ready to use, then changing over to this disk is said to be changing while hot. This means that the volume change takes place without the need for shutting down the PC to affect the change. Since Windows 95, devices such as USB pen drives have been **hot swappable**, but they are harder to replace an internal disk drive. The disk drive is located on disk startup after a BIOS scan. However, here, especially with servers such as Server 2012, the disk exists in a powered state, ready for use, and is called when needed. The disks exist in a group referred to as the **primordial** and can be added to existing volumes as they expand by the OS automatically.





# Solid state/flash drives

In this next section we are going to take a look at all of the removable media used for rich media storage, such as those used interchangeably between a digital camera and laptop / PC.



# Compact flash

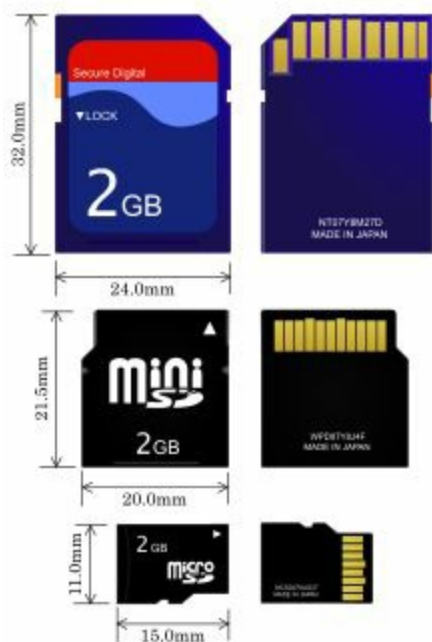
This format is common within digital cameras. It was developed by SanDisk in 1994. It supports from 2 MB to 512 GB:





# SD

The SD card was launched in 1999 and is common to smartphones. It contains account information but also can be used as a file store. It typically supports 1 MB to 2 GB, up to 256 GB:



MiniSD and MicroSD with dimensions



# MicroSD

The MicroSD was released in 2006 and is also common for most digital devices, but is synonymous with smartphones. The MicroSD can fit into converters, which allow it to be used in MiniSD or SD formats.





# MiniSD

Similar to a microSD. This launched in 2003 and was capable of up to 256 GB.



# xD

This card was specific to Olympus and Fujifilm cameras. The Standard design, launched in 2002, was similar to the SmartMedia card, supporting 512 MB. Type M launched in 2005. It was slow to read and write but could store up to 2 GB. Type H is identical to M and supports the same size, but is faster:





# SSD

A Solid-State Drive and a USB pen drive (also referred to as a **flash drive** or **flash stick** since it is quick to install and access) are simply printed circuit boards with ROM chips capable of storing data after the power is switched off or the device is removed. Solid State access times are extremely fast, so there is a benefit to using these where drive activity is common or performance is key. However, most modern SSD drives have a smaller capacity than traditional drives.



# Hybrid

This is a hard disk containing both mechanical and Solid State portions. This effectively enables two hard drives within one physical device. The Solid State is used to create a partition, which requires fast access, whereas the mechanical portion is for longer-term storage where access speeds are less of an issue.





# eMMC

This takes the hybrid analogy one stage further by embedding the multimedia controller card into the device itself. With earlier devices the drive connected to a controller card, which was responsible for the flow of data and where to access this data from (for example, the address space where the data was located, or block/sector/disk information). With eMMC, the controller is dedicated to supporting and managing the device it is part of. This is commonly found in tablets, PDAs, smartphones, and other integrated systems. It makes the entire disk and connection to it **plug and play**, whereas in the past we required a controller card which would manage an **redundant array of disks (RAID)**.



# RAID types

- **0. Striping:** Here the single disk controller is connected to two (or more) drives. The dataset to be saved is split into portions and each separate portion is sent to each drive at the same time. This therefore doubles the time taken to write data out to the disk. Striping provides a performance benefit, but all disks in the RAID array need to be present for the volume to work.
- **1. Mirroring:** This is the opposite of Striping. The data block to be sent is duplicated and sent out to two (or more) drives from the controller. There is therefore a second copy of the same data on the second disk, and both disks are live. Both disks make up the volume. If one disk fails, the volume can still be accessed through the disk, which is still live. However, there is no performance benefit other than the fact that no data is lost and a fault can be tolerated (referred to as **fault tolerance**). A variant of this has each disk connected to its own disk controller. Here, the controller card does not form a bottleneck.
- **5. Striping with parity:** Here, three disks are used. Two disk stripes are saved (A and B are different but make up the data to be sent out to the array). The data recorded (known as the **stripe set**) is put through a checksum algorithm and a unique number is generated, which can only be created from the exact pieces of data input into it. This is referred to as the **parity block**, or **parity bit** (although the number is usually large and definitely not a binary digit!).

Combinations of these RAID types are also possible. For example:

- **10. Mirrored set, then striped:** Here, we are using 4 disks in the combination: stripe data, stripe data copy, mirror of stripe A, mirror of stripe B.
- With this solution you get a performance benefit and immediate access to the volume in the event of a two-disk failure.
- **RAID 6** is a newer variant of RAID 5 using a second copy of the parity bit. The parity bits are cycled on each save, but it means that the volume can be regenerated in the event of two-disk failures, and the regeneration is considerably faster as more data is available in the event of one disk failure. RAID 6 uses four disks in the set.
- Windows Server 2012 supports an alternative called **Disk Mirroring**. Here, a mirror set with two-way mirroring requires five disks: the original, the mirror to the left, the mirror to the right, and two parity disks.





# Tape drive

The tape drive system is used for offline backup. It is not intended to be used online as a data accessing solution.

The A+ certification used to cover various different physical tape types and capacities, but this is now redundant as most external backups are either done to an external hard drive or to the cloud. **Digital Audio Tape (DAT)** is still, however, used as a common backup format.

The main server was located in the reception area. Each evening the receptionist placed the backup drive into the bay and then went home. Two years later, the network fails and the server needs to restore data from the tape drive. A consultant has been hired to retrieve company accounts. The retrieval fails.

Why is this?

- A) The tape was being added but a backup was never triggered
- B) The tape was dirty
- C) The tape was worn
- D) There was never any data being stored to the tape.
- E) The receptionist was not a member of the Backup Operators group in Active Directory

The correct answer is actually A. The receptionist was never trained, but also was not a member of the Backup Operators group. Either of these would stop her from being able to physically back-up.





# Media capacity

Thus far we have described the look of the physical media but not what it can contain:

- **CD:** As previously detailed, a single side CD is 700 MB.
- **CD-RW:** Rewritable CDs were also 700 MB approximately per side and per layer.
- **DVD-RW:** DVD sides were 4.7 GB per side and layer. The disk can be rewritten.
- **DVD:** DVD sides were 4.7 GB per side and layer.
- **Blu-ray:** Blu-ray sides were 25 GB per side and layer.
- **Tape:** As an example, Sony DAT tape is capable of 320 GB.
- **DVD DL:** DVD DL disks are capable of 8.5 GB.
- **DVD + or - RAM formats:** There is little difference between the + or - formats. The disk is designed to work in the appropriate player designed for the format; however, both formats are interchangeable. In fact DVD+ refers to enhancements in some players, whereas DVD- simply means the general DVD format.



# Video training

To summarize this section I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **An Overview of Storage Devices:** <http://www.professormesser.com/?p=19367>
- **An Overview of RAID:** <http://www.professormesser.com/?p=19373>



# Summary

In this first part of the first module we have covered a lot of ground. In fact, if you are spinning by the sheer amount of data you have taken in I can understand and empathise. It is a lot to take in in one reading so I encourage you, as with a Japanese meal, to take this in small sessions so that you can properly research, contextualise and understand the various objects here and how they are used.

You have the disadvantage--I'm old! At 41 I saw this stuff be introduced first-hand. We now live in an age where this technological 'failures' (as some are, even though they at their time were considered the best thing ever created) actually form our history. Yes, it is good to contextualize them--know where you have come from to know where you now are, then to aspire to where you are going, but more importantly CompTIA also recognize the history lesson for a good reason - you have to support technology that may well be 20 years old.

In the next section we will broaden our understanding by looking at wider network, printer and mobile hardware factors.



# Hardware 1.2 (901.1)

So far, we have looked at various system hardware components - what they are used for, the firmware (software) used on them and also a variety of backup media. In this section of module 1 we will look at processors, connectors, ports and display output. We will then look at bespoke systems for example High-end Rich Media Video Editing systems, or Graphics Rendering stations to see how their requirements exceed normal expectations. We then look at external peripheral devices that can further enhance productivity, or even gameplay!





# **901.1.1 Installing various types of CPUs and apply the appropriate cooling methods**

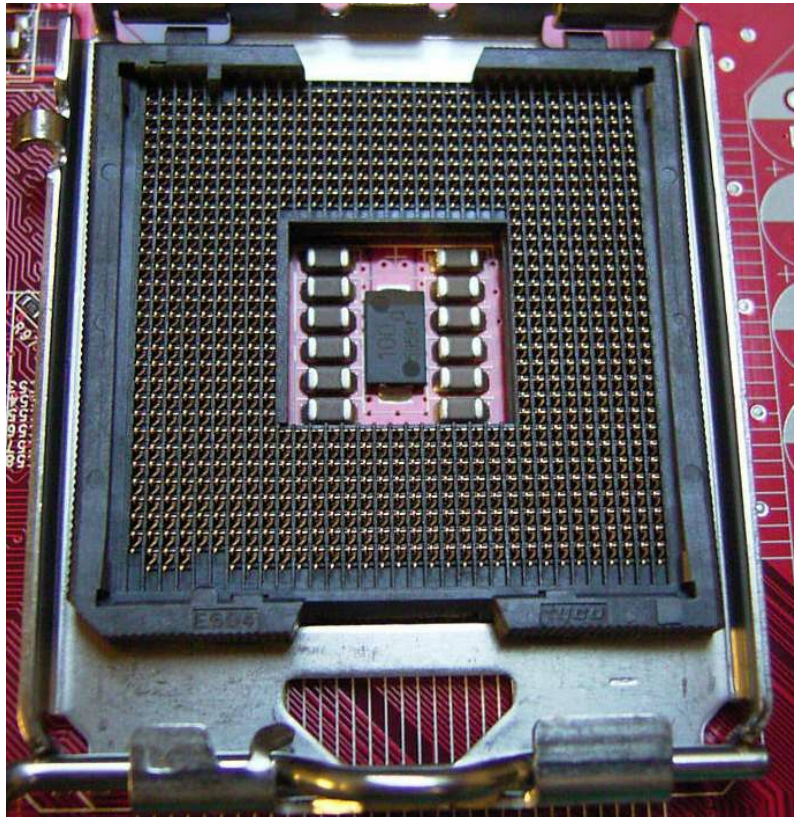
This section focuses solely on the processor and lists all of the known active processors from the Pentium 1 family to modern processors, so spans approximately 20 years of development. Your task is to determine a timeline and to learn the different types of processor available from the two main manufacturers--Intel and AMD. We will consider the socket types, what they look like, how many pins they support, and for which architecture they are used. We will then consider some of the features and characteristics of the processor. Finally, we will look at cooling technologies required to keep the processor functioning without burning out.



# Socket types

The exam will need you to have a time reference - know which processors supersede which other, older ones. For the purposes of clarity they have been placed in timeline order below. You need to know the number of pins, any interesting features of the processor type and whether it is **Pin Grid Array**, or **Land Grid Array**. You do not need to know any further information than that (such as the specific difference of the Piledriver series).

- **Intel:** Intel typically use Land Grid Array sockets, where the pins are on the socket:



Land Grid Array (LGA)

- **775:** Socket 775 / Socket T (Tejas Core) support Intel Pentium 4 Prescott, Pentium D, and Pentium Extreme Edition processors. The Celeron and Celeron D processors also use socket 775. The 775, unsurprisingly, has 775 pins. This type was popular in 2004.
- **1155:** Again, a successor to the 775 and looking similar to the 1156; there are a few pin-configuration differences to key the processor and avoid placing the 1155

into an 1156 socket. It is associated with the Intel Sandybridge and Ivybridge models.

- **1156:** The 1156 is also known as Socket H. This featured in 2009 and is a successor to the 775. One interesting fact is that the processor also contained the Northbridge chip, integrated onto the processor rather than existing as a separate chip on the motherboard.
- **1366:** The 1366 has 1366 pins on the socket. It is an LGA processor and is the successor to the 775. It appeared in 2008 and is synonymous with the Intel Core i7.
- **1150:** The Socket H3 has 1150 pins. It was a successor to the 1155 and was released in 2013. It is associated with the processor brand names Haswell and Broadwell.
- **2011:** Known as Socket R and with 2011 pins, the processor supersedes 1366 and 1567. It is used with high-end desktops and servers. It has excellent support for PCI Express (40 lanes), meaning that graphics-intensive processing can be handled by the CPU and GPU with little to no delay in data access. It uses Intel QuickPath (QPI), allowing interconnection between CPUs.
- **AMD:** AMD, conversely, make Pin Grid Array sockets--the pins are located on the processor itself, not on the socket. AMD led to AMD v2, but we will start the conversation from approximately 2009 with v3 - the AM3.
- **AM3:** The AM3 has 940 pins and is keyed to fit the AM2 and AM2+ sockets. However, if you did want to run an AM3 processor on the earlier motherboards a BIOS upgrade was needed to support the processor.
- **AM3+:** The AM3+ uses 942 pins, but the socket is more interesting here as you can use the older AM2 processors in the AM3 socket. The AM3, due to its adaptability and compatibility, has a long shelf-life within the marketplace.
- **FM1:** Released in 2011, the FM1 has 905 pins. It supports AMD's newer 10h / A-series architecture, which provided faster speeds and also faster access time with better support for DDR3 RAM. Finally, the PCI Express controller chip was actually integrated into the CPU processor.
- **FM2:** Released in late 2012, the FM2 has 904 pins and is similar in architecture to the FM1. The one-pin difference did lead to a number of mistakes where an FM1 was forced into an FM1 socket (an expensive mistake to make), so there is a physical keying difference. It is synonymous with AMD's Piledriver brand of processors.
- **FM2+:** Released in 2004 the FM2+ was a micro-processor. The pin grid array was smaller and it had 906 pins. Pin configuration was different and an FM2+ could not fit into an FM2 socket (and vice versa). This was associated with the Steamroller brand.



To revise these, it is best to visualize them. Review the Professor Messer videos listed at the following URLs: <http://www.professormesser.com/?p=19398> and <http://www.professormesser.com/?p=19403>.



# Characteristics

This section will look at some of the measurements you need to understand in relation to the processor using metrics such as their speed, number of cores, cache size, architecture and especially if they can handle virtualization.





# Speeds

The older processors were measured in megahertz, but it is now common to see speeds measured in gigahertz. On its own, the speed at which the CPU processes information forms only a small part of the overall speed of the PC as there could be a series of bottlenecks as different parts of the PC operate at different speeds. It is important, therefore, to consider the movement of data and the speed at which that data travels for all components that make up the PC, giving a holistic PC speed, rather than relying on the CPU speed and announcing that 'it's a 3.4 GHz system', as is common to see in PC marketing.

The processing speed is also dependent on the system's clock speed, as it is a combination of processes per cycle and the speed at which data travels, which gives us our processor speed.



# Cores

The number of cores affects the number of parallel calculations taking place at any one time. A 4-core CPU is capable of performing four separate calculations at the same time--one on each core.



# Cache size/type

It is now common to see the level 1 cache and also, possibly, the Level 2 cache integrated onto the processor itself, rather than existing on the motherboard. The Level 3 cache is a shared cache and can be accessed by all of the cores.

As complexity evolves over time, the number of cores has increased (for example, 16 cores on one processor). Combine this with NLX motherboards and blade servers capable of hosting 8 / 16 CPUs on one motherboard within the blade and the processing power available at enterprise level is tremendous.

Why is cache important? Sharing data across the cores and each core having a memory buffer will significantly increase the throughput of data we can send into a CPU.



# Hyperthreading

Intel is famous for being the leading processor manufacturer over AMD, as early on, it recognized that the CPU had to be capable of receiving a lot of data as quickly as possible and that the main problem was that data is fed first into memory, then into the CPU (even if the Northbridge directs the data from, say, the Southbridge to go directly into the CPU, or in the case of the PCI Express bus for graphics), the CPU ends up doing a lot of waiting until the memory is ready to send or receive data.

Hyperthreading, therefore, is a technology that allows one CPU to work as though it is in fact two separate, physical CPUs. By splitting the load, data can be calculated in one thread and new data written into the other thread. Hyperthreaded CPUs provide up to 30% improvement over a non-hyperthreaded CPU (such as the AMD range), which explains why Intel has the edge over AMD for a processor marked as being at the same processor speed.

Not all operating systems support hyperthreading, but support is built in from Windows XP and higher.

Think of hyperthreading as being a little bit like lanes on a motorway--the first lane is in use, so the car, rather than waiting in the queue in the first lane, moves out into the free space in the second lane.





# Virtualization support

Virtualization is the process of running a software instance (a virtual machine) and allowing this virtual machine to have access to the same hardware resources as the host physical PC. The virtual PC relies on a management layer referred to as a **hypervisor**, whose job it is to convert commands from the virtual PC into instructions so that it can interact with the real-world hardware, but also, conversely, to allow the virtual PC to know the capabilities of the hardware it is installed onto. If you were to check the device manager, or a system information report in a virtualized PC, you often get emulation for real hardware, this emulation is provided by the hypervisor.

However, the motherboard must support virtualization and for this it is essential that the BIOS configuration is set to enable virtualization support (Intel's VT, or AMD's AMD-V).

If virtualization support is not enabled, some limited hardware capabilities can be emulated, but not all of it, and certainly not the advantages of the more recent and complex processors.



# Architecture (32-bit versus 64-bit)

An important consideration is the PC's architecture. Physically, the 32-bit processor only contains pins around the edge of the processor, whereas the 64-bit is completely filled (on the base of the processor) with pins. The 64-bit architecture is capable of carrying much larger number sizes and therefore, the calculations that can be performed are considerably more complex; however, these binary calculations are being performed extremely quickly, so the performance benefit of 64-bit over 32-bit from this perspective is clear.

In simple terms, a 64-bit bus can send twice as much information as a 32-bit bus (in terms of data lanes used), but the number is in the order of  $2^{32}$  (4,294,967,296) compared to  $2^{26}$  (67,108,864).

If you are using 64-bit, the hardware must all be 64-bit (although some systems support backward compatibility for older 32-bit components). To benefit from the 64-bit architecture, the Operating System should also be 64-bit to be able to send and deal with the larger numbers required. Drivers also need to be 64-bit where hardware is also 64-bit. Applications should typically also be 64-bit versions, although here, the OS does have backward compatibility for 32-bit applications as well.

Take a look at your C: drive. On a Windows OS, you will find a `Program Files` folder. On a 32-bit system there is just the one and this stores all of your 32-bit applications. However, on 64-bit systems there are two folders--`Program Files` and `Program Files (x86)`. On the 64-bit system, `Program Files` refers to 64-bit applications and `Program Files (x86)` refers to 32-bit applications.

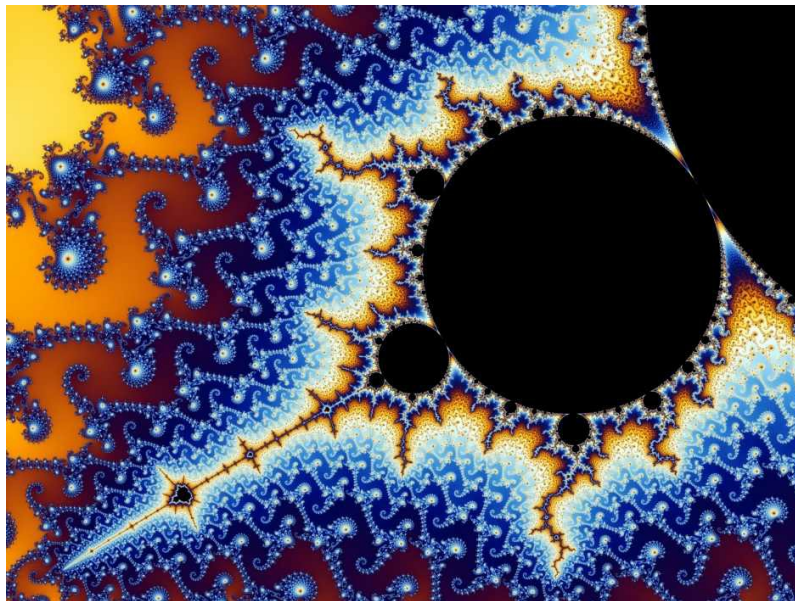


# Integrated GPU

By integrating the PCI Express Graphics Processing Unit onto the processor, the graphics data read-write delay can be eliminated. However, this is not a trade-off for a separate, highly powerful graphics card, which was able to dedicate to all graphics processing, and by so doing remove this load from the processor, allowing it to concentrate on other processing calculations.

Older readers should not confuse this concept with shared video memory. There, a portion of RAM was allocated for use by the video card as additional graphics RAM, but this took away from the badly needed RAM at a time in computer history where domestic PCs only had 2 to 4 GB RAM to work with anyway.

I am reminded of the parallel with the Maths Co-processor chip versus the logic card. Back in the 1990s I was a big fan of creating Mandelbrot images - computer images created from a repeating formula. These often took a long time to render; however, with a logic card, the mathematical calculations required behind the scenes to generate the image took far less time because I had a dedicated logic card capable of dealing with this large amount of mathematical calculation. A Maths Co-processor chip similarly took the load from the main core and dedicated to mathematical calculations:



A Mandelbrot image



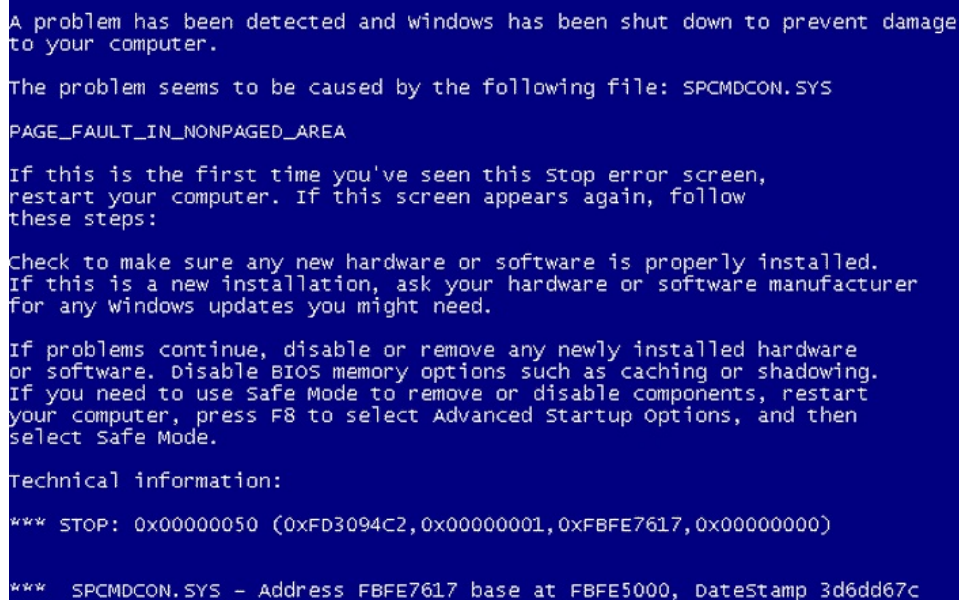


# Disable execute bit

Do you remember the **blue screen of death** synonymous with Windows 95? Have you noticed how much more stable systems are now, since XP and higher? There is a reason for that and one of the enhancements concerns the Disable execute bit.

Your CPU is responsible for determining which address spaces code will be written to in RAM and will then be run. It can also define specific other areas where code cannot be run. Modern operating systems (Windows XP and higher support this) have a feature called 'Data Execution Prevention,' which reads the execute bit as defined by the CPU to find out which areas of RAM are safe for code to be executed.

A virus will potentially try to run code in areas in RAM that have been defined as where code should not execute, and by doing so will cause the system to crash as other live, vital data is wiped over. DEP and the execute bit allows the OS a degree of protection to prevent this from happening:



```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The problem seems to be caused by the following file: SPCMDCON.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

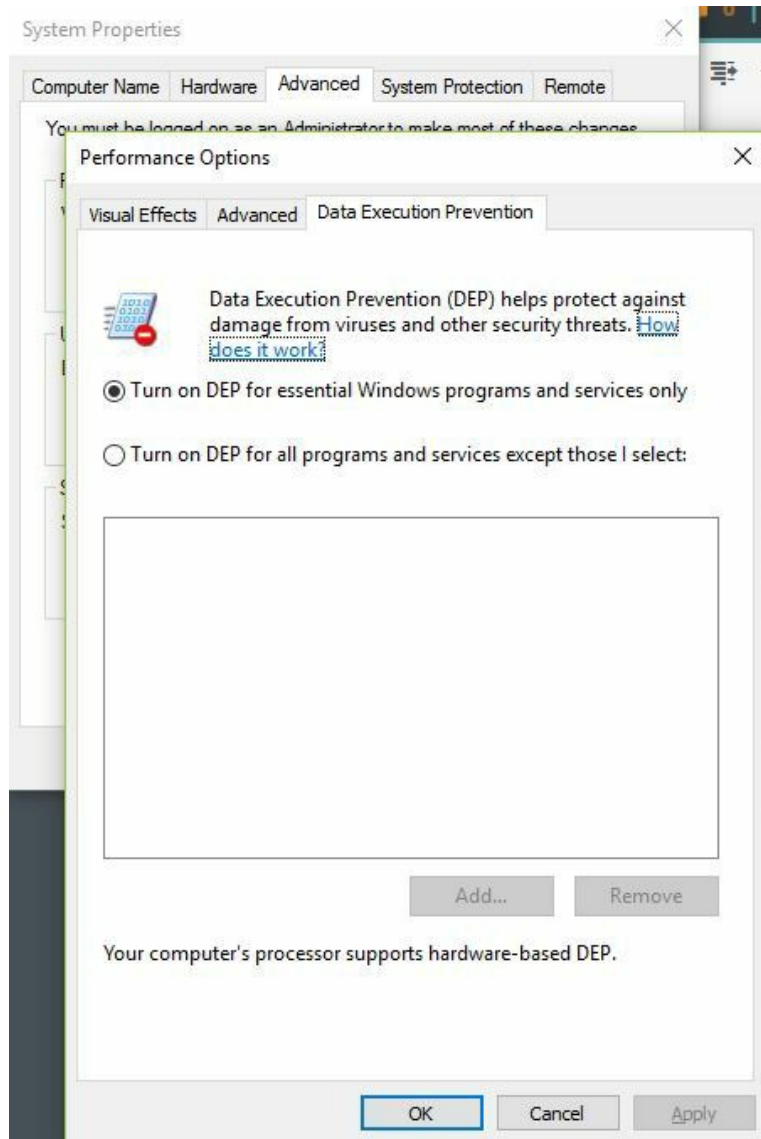
*** STOP: 0x00000050 (0xFD3094C2,0x00000001,0xFBFE7617,0x00000000)

*** SPCMDCON.SYS - Address FBFE7617 base at FBFE5000, DateStamp 3d6dd67c
```

Windows XP Blue Screen of Death Stop Error page

DEP is enabled by default. To get to the DEP section on a Windows system (XP and later), go to the Start button | Control Panel | System | Advanced System Settings | Advanced | Performance settings | Data Execution Prevention:





Data Execution Prevention



# Cooling

From a practical perspective there are also physical components of the processor that we need to watch for. This section will cover some of the supporting physical hardware used with CPUs.



# Heatsink

The heatsink is a piece of metal attached to the top of the processor. It is deliberately crafted to have a high surface area (similar to a radiator), so the heat is dissipated across the device.



# Fans

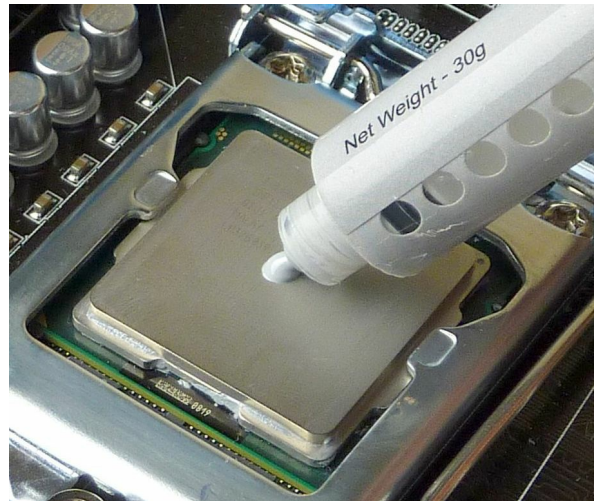
The heatsink fan is a 12 V DC fan mounted above the heatsink. Its job is to move hot air away from the heatsink so that other, colder, ambient air can be heated by the heatsink.





# Thermal paste

The problem with the concept of the heatsink is that it physically has flaws. There will be parts where the heatsink and processor top plate do not exactly match. The idea of the thermal paste is to add a medium (a grout), which is not heat-sensitive and will fill any air gaps that will otherwise be present between the heatsink and processor plate:



Applying thermal paste to the processor Liquid-based



# Liquid-based

One of the better solutions is to put the entire PC into a heat dissipating solution. One possible solution is to submerge the PC into an electrolytic-friendly and non-conducting solution.



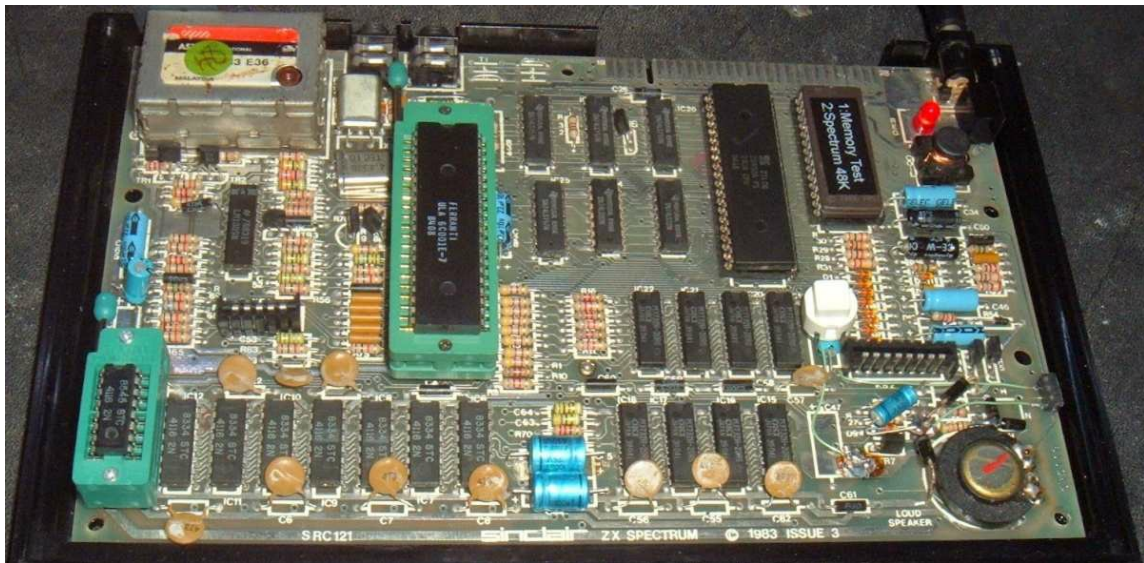
In this video we see the PC fish tank born! (from Puget computers): <https://www.youtube.com/watch?v=PtufuXLvOok>



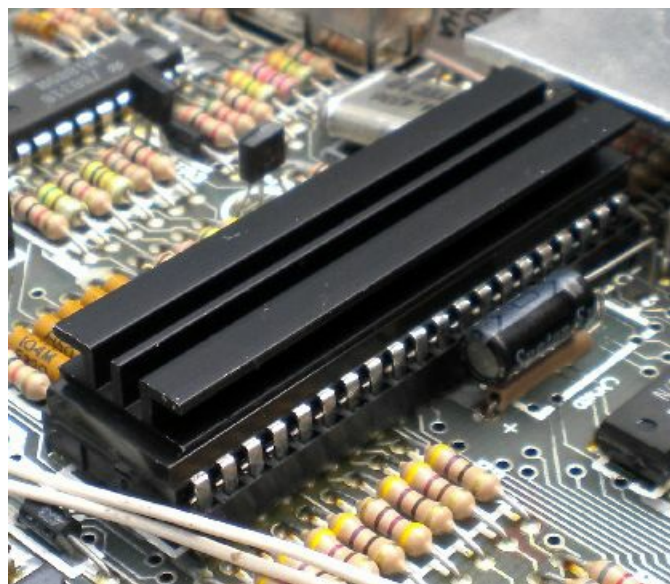
# Fanless/passive

Passive cooling implies no active component to move the heat away from key areas. It is a building-design approach where heat is naturally dissipated through the structure without the need for active cooling to move the heat on from one component to another.

The ZX Spectrum had an iron block one inch preceding the mainboard - all heat generated was channeled into this block. While there was no cooling, the block took a long time to heat:



An early ZX Spectrum exposed (without heatsink)



Sinclair ZX81 with heatsink

Passive cooling is also synonymous with throttling the processor - limiting the speed at which it runs so as not to produce excess heat.



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **An Overview of CPU Socket Types (7:14):** <http://www.professormesser.com/free-a-plus-training/220-901/an-overview-of-cpu-socket-types-2/>
- **Understanding CPU Characteristics (10:26):** <http://www.professormesser.com/free-a-plus-training/220-901/understanding-cpu-characteristics-2/>
- **CPU Cooling (5:52):** <http://www.professormesser.com/free-a-plus-training/220-901/cpu-cooling/>





## **901.1.2 Comparing and contrasting various PC connection interfaces, their characteristics, and purpose**

Ok, so we now know what is inside the box. How do we connect other peripherals and external devices to it? There is a variety of physical and wireless connection types, which are explained here. Along with this, we will look at the characteristics of the connection types, such as whether or not the signal is analog or digital. We will also look at the data transfer speed used and the frequencies available, as applicable.



# Physical connections

This section will introduce the various external connection ports you will need to memorise, especially their timeline and relative speeds.



# USB 1 versus 2.0 versus 3.0

USB 1 and 2 look physically similar. Both share the identical USB A port. USB 1 can run over a cable distance of up to three meters. USB's cable run is five meters. USB 3 is physically significantly different, as we will see following.

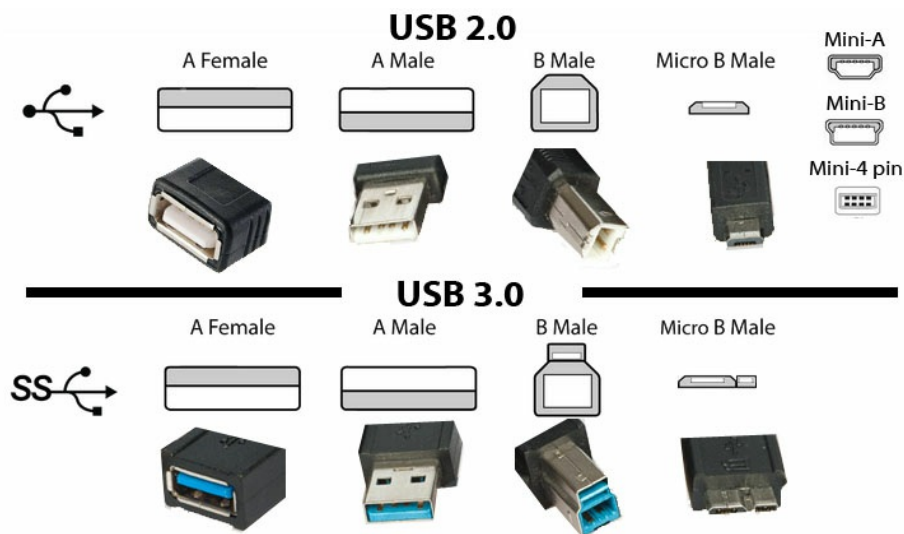


# Connector types - B, mini, and micro

At the other end of the cable, the USB B or micro-B plug is used to plug into the device.

USB 3 is distinctive for two reasons - the base plastic plate within the port is a distinctive blue color (always) as opposed to the white, or black, for USB 1 and 2. Also on the USB B end, there are actually two ports, therefore looking physically different to USB 1 and 2's B-port.

The USB 3 micro-B plus also uses a different set of connectors. USB 3 is therefore not physically backward compatible with USB 2, although USB 2 is physically backward compatible with USB 1:



USB 2 and 3 ports





# Firewire 400 versus Firewire 800

Firewire 400 (Alpha mode Firewire) is the IEEE 1394a standard. It transmits in half duplex mode at speeds up to 400 Mb/s. Firewire 800 (Beta mode Firewire) is the IEEE 1394b standard. It transmits in full duplex mode at speeds of up to 800 Mb/s.

The Firewire 400 comes in a 4-pin and 6-pin version. The 6-pin version is designed to send supplementary power to the device (so could be used to power a webcam, for example). Firewire 800 is a 9-pin cable:

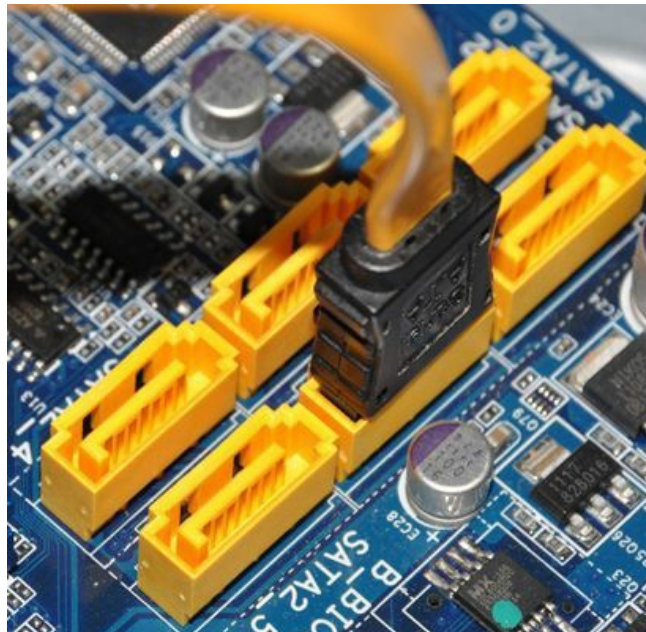


USB versus Firewire and Thunderbolt ports



# SATA1 versus SATA2 versus SATA3, eSATA

Serial AT Attachment SATA 1 ran 1.5 Gb/s over one meter. SATA 2 transmits at 3 Gb/s over the same distance. SATA 3 transmits 6 Gb/s over the same distance. These are therefore used in short-distance data travel such as to connect the internal hard disk drive to the disk controller card / motherboard. These are referred to as **internal** cables:



SATA port and data cable (internal)

**External SATA (eSATA)** supports the same transmission speeds, but over a cable length of two meters. This is used to connect storage hardware that is external to your PC:



eSATA port

Note that it is now possible to come across combination eSATA and USB ports.



# Other connector types

From these key ports we are now going to look at an array of other video ports which are also essential to know.

- **VGA:** The Video Graphics Array was a 12-pin analog RGB signal used to connect to CRT monitors. The VGA standard is an 640x480dpi resolution and was able to provide 16 or 256-color pallets. It was replaced by Super-VGA in the late 1980s. This second cable requires 15 pins and became the **Video Electronics Standards Association (VESA)** standard. SVGA can support 1024x768 dpi with a 256-color pallet.

The term VGA is used interchangeably to refer to the various graphics arrays that make up the suite, and for this reason the term VGA is often used to refer to the SVGA cable rather than the original VGA cable.

The SVGA cable is quite distinctive. The plug is always often blue, with two locking screws to hold the plug tight in place. The pins are arranged in three rows of five pins. The plug is D-shaped (for example, DE-15):



DE-15 plug (SVGA)

- **HDMI:** The successor to the VGA and DVI port, **High Definition Multimedia Interface (HDMI)** carries a high-definition video and audio digital signal. Standard HDMI cables support 720p and 1080i. High Speed HDMI supports the newer 4k and 3D systems.

HDMI now supports color depths of 1 billion colors (known as **deep color**), also 30, 36, and 48-bit color depths.

With version 1.4 HDMI can also support the sending of ethernet frames between the PC and TV, making TVs internet-enabled without the need for extra cabling. The cable must confirm to the HDMI ethernet Channel specification.

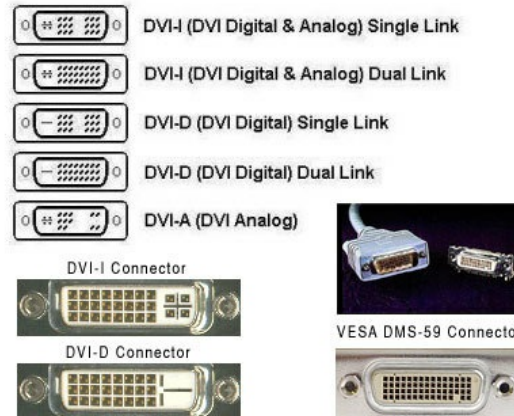
HDMI is compatible with DVI--digital and dongles are available to adapt DVI-D to HDMI and vice versa.

HDMI uses 19 pins and is D-shaped:



HDMI plug and socket

- **DVI:** The Digital Visual (Video) Interface was developed to be a common standard for video. It supports either analog signals or digital signals, with a third pinout system capable of taking either digital or audio. It supports 1 or 2 links, thereby using the second link for higher resolutions. The maximum resolution possible from a single link is 1920 x 1080, which can then be increased to 2048 x 1536:



DVI connectors

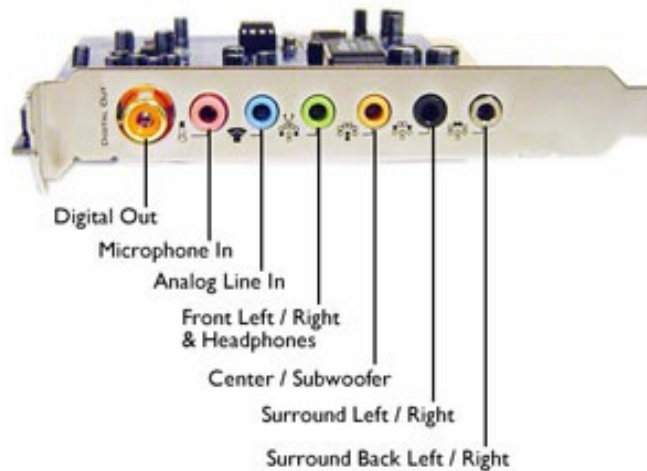
- **Audio:** Audio cables fall into three different categories:

Stereo 3.5 mm mini-jack (Tip-Ring-Sleeve connector) connects both stereo channels and a shared earth wire so that both devices are 'balanced' (sharing the same electrical "earth" voltage), thereby negating interference caused by the electrical differences between the devices. It is commonly used to connect a speaker or headphones to the PC. The signal is analog. For inputs, both the microphone and line-in ports also use 3.5 mm mini-jack connections.



The port color coding denotes the stereo signal being sent. Typically, on a Dolby / 5:1 channel audio system, lime green denotes front stereo out, pink is for the microphone, sky blue is line-in, black is the back stereo channel, and there is a yellow port for the subwoofer (bass) channel.

Depending on the manufacturer you will also find a yellow 3.5 mm mini-jack, or more commonly an RCA port, used to input a digital audio signal:



Sound card ports

With composite video, 3 RCA ports are used to carry the video (yellow), Stereo pair main (white) and stereo pair second channel (red):



Composite ports

- **Analog:** With the exception of the RCA digital out audio port, all other ports listed in this section carry an analog signal.
- **Digital (Optical connector):** For either video or audio, fibre can also be used,. Fibre-optic leverages extremely fast data transmission speeds between devices. Both HDMI and optical can send Dolby Digital quality sounds, unlike RCA

Composite. Optical tends to be used to connect the media server to a sound bar, or amplifier where HDMI is not given as an option. Optical does not support Dolby TrueHD, or DTS sound systems:



TOSlink audio cable

From here we now focus our attention on Network ports - a vital section of the book covered again in the next module:

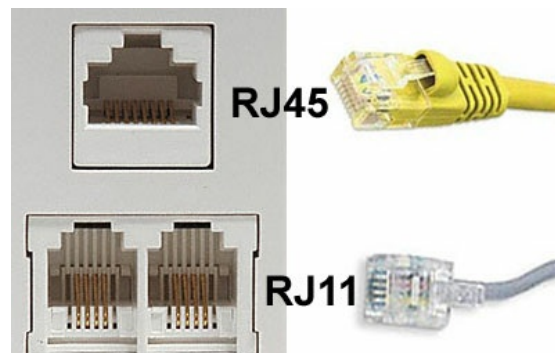
- **RJ-45:** Registered Jack type 45 is the most common network port. This is the standard ethernet connection port as found on NICs, Hubs, Switches, and Routers. The RJ-45 is the common connectivity standard for connecting any network device. It consists of four pairs of twisted-pair wires arranged in the configuration 568A or 568B at both ends. This would create a straight-through or patch cable capable of adding the device to the existing network.

RJ-45 is described as an 8P8C technology, meaning that all wires are connected to a pin, connecting them to the device. In theory, all eight wires could be used. This is in contrast to RJ-11, or the RJ-45 loopback plug, where only two wires are actually used (of 4 available in the plug):



RJ-45 port

- **RJ-11:** Registered Jack type 11 is a small, clear, plastic plug with four gold/copper pins on one side and a locking clasp on the other. Of these, only two are typically used for standard analog phone networks, although all six are usually wired. For the UK, it is common to only see four wires in use. The RJ-11 is used to attach a serial connection to a device such as a managed router, but is more commonly used for connecting to a modem to allow connectivity between the PC and the telephone line. A second RJ-11 line is used to plug in the telephone as a monitor device and also to enable the telephone to operate normally when the modem is not in use:

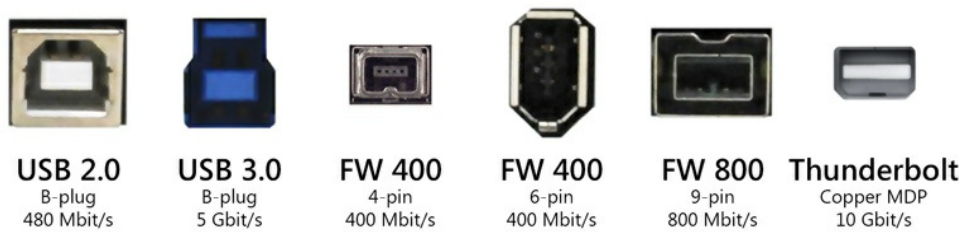


RJ45 and RJ11 ports showing the pin differences

In the UK, **British Telecommunications (BT)** has held the monopoly of the telephone network throughout the 1980s and 1990s. BT developed their own equivalent phone connector plug based on RJ11 but has a wider connection. Typical ADSL filters till have a BT jack and BT female input, but will use an RJ11 input for the digital DSL signal.

- **Thunderbolt:** A smaller version of DisplayPort, the Thunderbolt was a joint project between Apple and Intel. The DisplayPort v1 technology was combined with PCI Express x4 and was a cheaper option than DisplayPort, capable of transmitting files or video.

Thunderbolt has 20 pins and, as with USB, can also transfer power and data, as well as video signals:



USB versus Firewire and Thunderbolt ports



# Wireless connections

From wired connections we now consider Network wireless connectivity:

- **Bluetooth:** Bluetooth is a reliable, easy-to-use, ubiquitous facility now present in most modern smartphones and laptops. Bluetooth enables point-to-point connections with one other device, such as a Bluetooth keyboard connecting to a smartphone, and works by sending radio signals to the connected device. Bluetooth operates on the 2.4 GHz band and typically would send 1 Mb/s over 10 meters, although recent versions of Bluetooth are being developed that increase the speed and range at reduced power. Bluetooth is the connection system of choice for local gadgets or personal accessories (for example, a Bluetooth headset, earpiece, or hands-free kit).

Bluetooth requires a common PIN code from both parties, does not need a direct line of sight as it is an omnidirectional radio signal, and can send to up to 10 meters.

- **RF:** There are two key frequencies used by common wireless protocols:
  - **802.11a:** Used from 1999, this earliest protocol transmits with a peak data rate of 54 Mb/s using 5 GHz. It was highly susceptible to signal interference from walls.
  - **802.11b:** This early protocol can transmit longer distances than a and is less susceptible to signal interference from walls or objects. Its peak data rate is slower at 11Mb/s. It transmits at 2.4 GHz.
  - **802.11g:** More recently, **g** has surpassed **b** as the main wireless protocol for public use. It can transmit long distances and provide the stability benefits of **b** while providing peak data rates of 54 Mb/s. **g** uses the 2.4 GHz band.
  - **802.11n:** This makes use of a Multiple Channel system (usually two but can be up to four antenna within the station). It can transmit on either the 2.4 or 5 GHz bands, offering peak data rates of 600 Mb/s.
  - **802.11ac:** This was released in 2013 allowing multi-station throughput at 1Gb/s and a single link of 500Mb/s. It has a wider bandwidth than n with 80MHz mandatory, but 160MHz possible. It has up to 8 MIMO streams as compared with 802.11n's 4 streams and supports downlink multi-user MIMO allowing four clients to connect to the transmission at the same time. 802.11ac is an enhancement using a, g or n transmission types.
- **Channels:** A wireless channel is a specific range used for transmission. The

channel is set on the WAP and devices will determine the best channel to use (although some end-device wireless NICs allow the user to also set the channel that will be used). The range is 22 MHz, so is quite a narrow band. The bands are numbered and each overlap slightly. Channel center frequencies in the 2.4 GHz range start with channel 1's center frequency at 2.412 GHz, up to channel 14 at 2.484 GHz.

- **Goodput:** Wireless packets are considered 'good' if they can be used by the end device (the system). A weak packet may mean that not all of the information is received; equally, interference or crosstalk may affect the transmission, leading to the packet having to be dropped and sent again by the sending WAP. Goodput is the throughput (at Application level of the OSI model). It is a measurement of the quality of data transmission based on the efficacy of the data transfer (in that it can be used by the system).

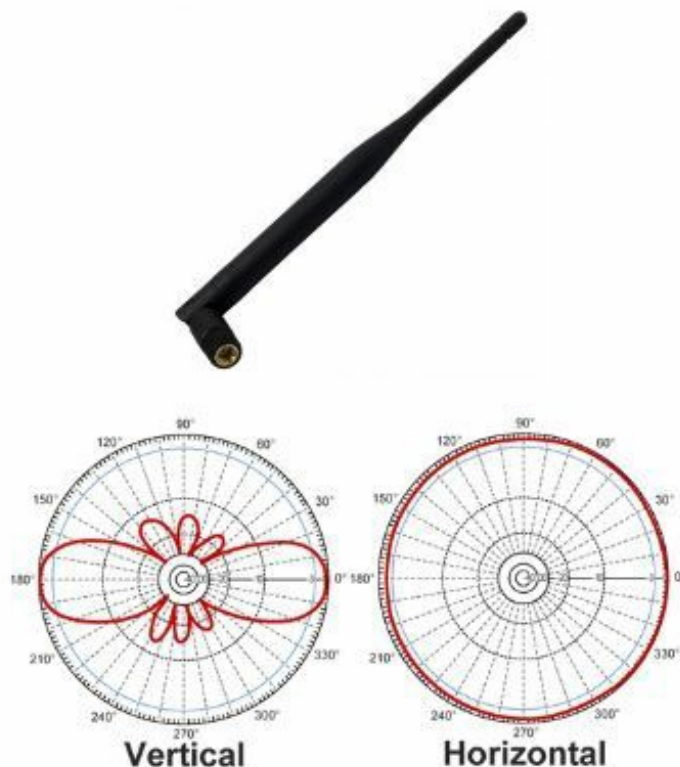
If we were transferring a file with high goodput, there would be no need to resend corrupt data packets, so file transmission speed will be only as long as would be expected through the confines of the hardware and protocols used. We sometimes express the goodput as a percentage of the best possible time taken to transfer the file divided by actual time taken to transfer the file. Typically, however, goodput is represented as a ratio between the delivered amount of information and the total delivery time. We are aiming for the ratio to be low, or as close to 1:1 as possible.

- **802.11a-ht:** This refers to a wireless adapter with the physical type referred to as high throughput (high successful data delivery) and using the 802.11a protocol.
- **802.11g-ht:** This refers to a wireless adapter with the physical type referred to as high throughput (high successful data delivery) and using the 802.11g protocol.

Antenna placement is very important when configuring the network, as each WAP needs to be able to provide the greatest range possible with the transmission power selected. An antenna, as with an FM radio, is a metal pole raised from the WAP allowing airborne transmission of the radio wave. It is also able to receive other radio transmissions and to pass these to the WAP for processing.

When attempting to connect a trunk line between two Wireless Access Points, the antenna must be placed so that both antenna are transmitting within each other's range. A Unidirectional (Yogi) antenna is used to direct the signal to the receiving WAP station.

An omnidirectional antenna provides an equal range in every direction:



An omnidirectional antenna. Range diagram of the antenna

A unidirectional antenna provides a highly focused arc, able to achieve slightly longer distances, but generates the signal in a specific location (as with a microphone).

- **IR:** Infrared is a relatively slow communication system which, as with a remote control pointing to a TV, needs a direct line of sight to the receiver. The maximum distance of IR is one meter, making it impractical for all but PAN networks, for file sharing between two smartphones; however, this is superseded by the more reliable and slightly more secure Bluetooth:
  - IrDA-SIR (slow speed) infrared supporting data rates up to 115 Kb/s
  - IrDA-MIR (medium speed) infrared supporting data rates up to 1.15 Mb/s
  - IrDA-FIR (fast speed) infrared supporting data rates up to four Mb/s
- **NFC:** Near Field Communication has become increasingly popular and no doubt you already are using it. Do you have a contactless bank card? I do. it provides a certificate file, which is read by the reader. This file contains bank transaction information specific to your bank card and proves that it is your card.

Smartphones now support bank-supplied apps, which also do the same thing, allowing you to use your smartphone as if it is your bank card. A good example of this is Airpay.



There is still a psychological and social barrier to contactless payment, especially in cities where the local population is not technically minded. Here, there are still concerns that you might pay for the shopping of the person in front of you, should you happen to walk past the till and get too close to the reader. This is, of course, untrue, as the NFC range is only a few centimeters - you have to hold your card over the reader for a few seconds before the reader will trigger and the card's ID is read. Equally, Airpay may be a little more complex to set up for a person who is not a regular phone app user.

Nevertheless, NFC has a foothold and is increasing in popularity. So to follow will be gesture control where, for example, I am waiting at a train station and see a poster for a concert I want to go to. I make a gesture such as to point my smartphone at the poster and a ticket is automatically purchased.



# Characteristics of wireless signals

The actual signal sent differs, also how the signal is read. In this section we will look at how the wireless signals fundamentally contrast. We will look at the distance limitations for each system as well as consider data transfer speed, signal quality and the frequencies used to send our wireless signal.

- **Analog:** The analog signal is a measurement of data values in a predefined scale, against time. The data stream is measured at set rates and each number sent represents something significant. Each number represents something. A musical scale may be considered as an analog signal as each note played can be represented as a note on a musical score. Alternatively, the ASCII table is a representation of text as Hex values.
- **Digital:** The digital signal is a representation of data using one of two values over time (0 and 1). The sending of data is not as complex or "rich" as analog. Therefore, considerably more binary digits, or BITS, are sent to represent the same value as would otherwise have been sent with one number, using analog. The binary signal, however, works very well with digital machines - 1 can be represented by a signal on a wire, irrespective of the strength (power) of the signal, over time. If we read a wire for a signal and taken measurements (for example, per second), which in turn represent our binary data, a number of these values (for example, sets of 8) are then converted back into something meaningful. For example, the number 240 can be expressed in binary as 11110000.

From an electrical perspective, the 8-bit sets can all be sent at the same time along a data bus. The data bus is a group of wires/solder lanes on the circuit board that can each send one bit at a time. Once received, the binary set is read as a set as a number representation and then used (for example, four live wires and four with no power all sent at the same time represents 240).

Digital data can therefore be sent at extremely fast speeds and can be understood and translated by the system very quickly.

The number of bits that make up the data bus defines the architecture of a computer. Most modern systems are 64-bit, meaning that it can take 64-bits to make up one number. Therefore, very large numbers can be sent at any one time from component to component.

- **Distance limitations:** After a certain distance, the resistance of the media itself causes the signal being sent to weaken. This is referred to as attenuation. The attenuation is dependent on the media and the type of signal we are sending. A separate matter to attenuation, but equally as unhealthy to the signal, is crosstalk - this is the fact that any wire, once unfurled, will act as an aerial and pick up other signals along the route. This additional data will overlay the original signal being sent across the wire, so the receiver cannot tell which signals are genuine. It is a little bit like listening to an analog radio set, with the reception slightly de-tuned so you get other stations - music cutting into the signal.

To minimize crosstalk shielding on the wire is essential; however, it will not eliminate the problem entirely. Crosstalk signals may be at different frequencies to the original signal; therefore, by filtering and focusing on the one specific frequency our original signal was sent on, we can ignore the other erroneous signals and still obtain our pure data. This is the same principle through which ADSL data can be sent across the phone line - voice data shares the same carrier media as the phone conversation, across the same phone line, but the ADSL splitter (filter) removes the voice portion of the bandwidth, allowing for a cleaner data signal.

- **Data transfer speeds:** Transfer speeds are measured in Mb/s or Gb/s. That is the number of bits sent per second. Note that when considering files, we refer to the file's size in bytes. To transfer from bits to bytes:



10 Megabyte/sec is equal to  $(8 \times \text{Gigabit/sec})/1000$ .  $10 \text{ Gigabit/s} = 125 \text{ Megabytes/sec}$ .

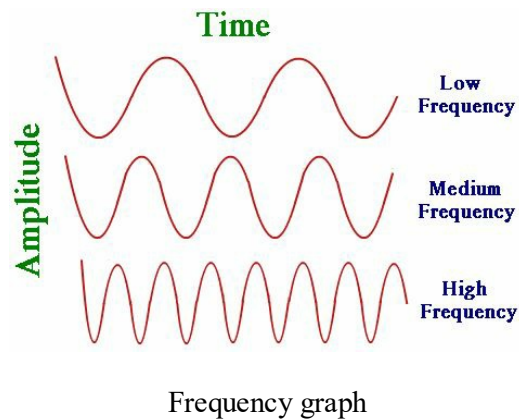
- **Quality:** Earlier on, we spoke about data quality. Here, we are referring to two things - how clean is the signal that is received and can it be read without errors?

To improve the amount of data we can transfer, the speed is determined not so much by the distance but the media and frequency selected. The higher the frequency, the more we can send, but the more error-prone the signal becomes.

TCP/IP and USB are both tentative and cautious protocols. They establish a base speed, which is a common slow speed that both end devices can definitely talk to each other on. They then gradually 'ramp-up' the speed until a maximum acceptable speed is reached. If confirmation packets are not received by the sender, then the speed is

considered to be too high, and the connection speed will drop. If there is heavy crosstalk, then again, the speed will drop until a happy medium is established.

- **Frequencies:** A frequency is the measure of a repeating event over time. For example, consider a sine wave. Measure the time taken for the wave to have traveled 360 degrees (a complete revolution) and for the same point to come back around. Frequencies are measured in cycles of repetition, per second, referred to as Hertz:





# Video training

To summarize this section I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Computer Interface Speeds and Distances (16:07)** : <http://www.professormesser.com/free-a-plus-training/220-901/computer-interface-speeds-and-distances-2/>
- **Wireless Interface Speeds and Distances (4:43)**: <http://www.professormesser.com/free-a-plus-training/220-901/wireless-interface-speeds-and-distances/>
- **Connection Characteristics (8:29)**: <http://www.professormesser.com/free-a-plus-training/220-901/connection-characteristics/>





## 901.1.3 Install a power supply based on given specifications

Before a system can be built, we need to determine how much power it will consume if all of the components and devices are being used at the same time. We add the power requirements and this will give us an understanding as to the capacity of power supply needed, but also if the motherboard is capable of supporting a system with such large power requirements. The increase in power will also increase the use of energy, and therefore the amount of heat produced, so our heat management is also influenced by our decision here.

Power cables are keyed and you have to purchase the power supply specific to the make of motherboard. For example, motherboards supporting AMD processors have AMD-focused power supplies with their own P1 and P2 connector blocks.

We will also consider the specifications of the power supply--physical size, the number of connector ports it supplies, the concept of a **dual rail**, as well as simply the output power (Wattage).



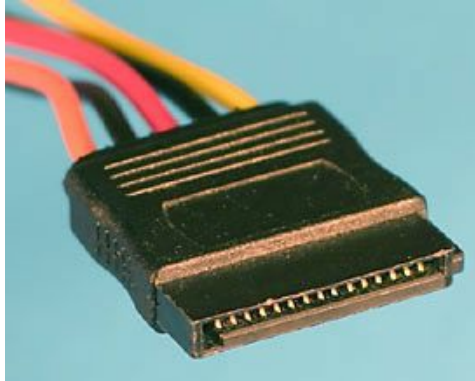
# Connector types and their voltages

In this section we will turn our attention into how to power each connector type we have mentioned so far.



# SATA

Serial ATA connectors supply 12, 5, and 3.3 volts. Many power supply manufacturers, however, do not include the 3.3 (orange) wire, so SATA hardware is designed instead to use 5 volts given the propensity of the 5-volt wire:



SATA 5-wire cable



# Molex

The 4-pin Molex is one of the original connectors and is still in use today. It is designed to connect to IDE hard drives or DVD-ROM, but is also used for general connectivity to support additional fans or case lighting.

The yellow wire carries +12 V, the black wire carries ground, and the red wire carries +5 V.

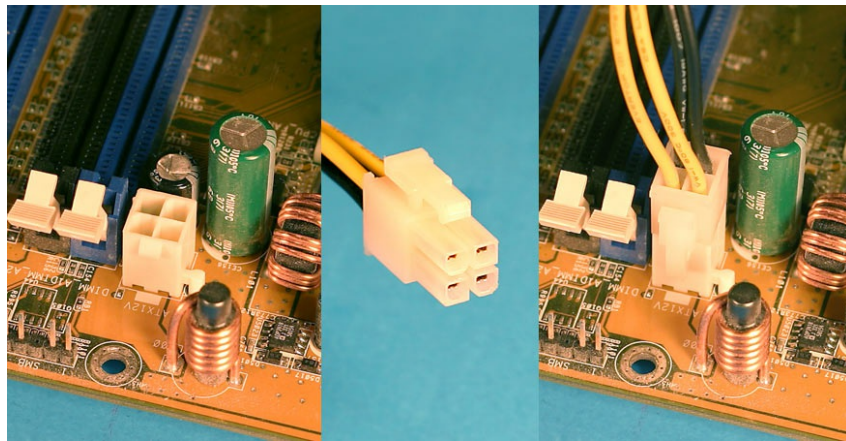




# 4/8-pin 12 V

Also known as **power socket 2** or P2 (P4 on ATX systems and, due to the black and yellow wires, sometimes coined the bumblebee connector and the Pentium 4 processor it used to power), the 4/8 pin connector block carries additional 12V power to the processing-intensive processor, and is also used to provide additional power for an integrated graphics card. The P2 socket is located next to the processor.

For dual-rail systems the additional 12 volts of power are supplied with this connector:

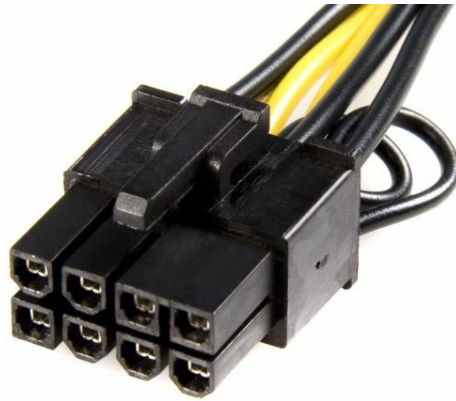


12v 4pin connector



# PCIe 6/8-pin

PCI Express video cards are power-hungry, often needing 75-300 Watts power depending on the complexity of the card. To assist with this, the 6/8 pin connector was designed to supply 12V power to the card. This cable is known as the **PCI Express Graphics (PEG)** cable . A typical 6-pin provides 75 Watts of power on a single rail:



PEG cable



# 20-pin

As from 1996, ATX manufacturers released the lower 3.3V rail. The P1 connector supplies the different power voltages to the various components on the motherboard. The motherboard needs both positive and negative voltage (voltage travels in the opposite direction on some parts of the board). The 20 pins supply the following:

- +3.3 volts (orange wire)
- Ground (black wire)
- +5 volts (red wire)
- -5 volts (white wire)
- +12 volts (yellow wire)
- -12 volts (blue wire)

The P1 also carried two wires to trigger a soft power on, doing away with the mechanical power switch supplying AC power to the power supply. The soft power button wakes the motherboard from a low-power standby state to full power.



# 24-pin

Later versions of the ATX board required 24 pins, where the additional pins would power the PCI Express section of the motherboard. This second pin type supports two rails for 3.3 V, 5 V, and 12 V.





# Specifications

Continuing with our study of voltage we now cover power dimensions as measured by how power is shared across the board, also by how we can determine power consumption across the system

- **Wattage:** Wattage is the measurement of power used to determine how much electrical power is needed to run the system. It is calculated by multiplying the voltage by the current:

$$W=VI$$

If you wanted to know what type of power supply you needed you would calculate the overall power consumption by adding the wattage of every device within the system.

- **Dual rail:** A rail refers to the circuitry that carries a specific voltage across the motherboard (for example, a five-Volt rail refers to all of the sections on the motherboard where five volts are used and transferred). A modern power supply may have four separate 12-Volt rails, each capable of independently carrying 12 Volts.

Current is important here as you want to balance the load on the power supply unit by equalizing this load across the rails, if possible. If one rail is overloaded, this may cause power interruptions or a system shutdown.

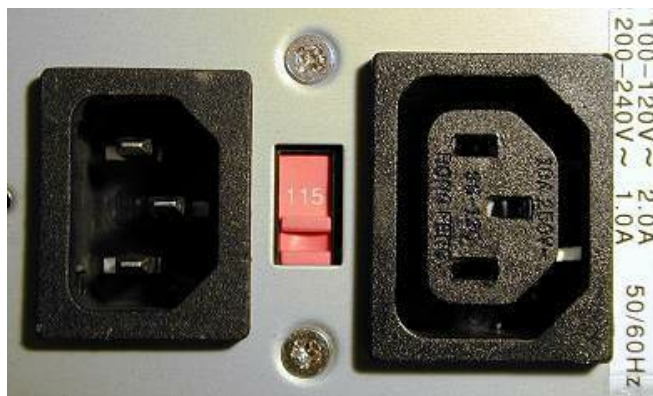
- **Size:** System size is a physical measurement of the chassis case and is based on the device width of 5 1/4 inches and 3 1/2 inches. Chassis size needs to accommodate good, well-managed airflow so that cold air is vented over the heatsink, and hot air is exhausted through the rear of the chassis.
- **Number of connectors:** The number of connectors available denotes the number of devices that can be added to one rail. While it is possible to use splitters to extend power to additional devices, be careful to equalize load across the connectors. If a device fails to power up (for example, the system works but the DVD drive does not light up) this could suggest that the device is underpowered.
- **ATX:** We have had a variety of revisions of the ATX standard since the development of PCI Express. Four, six, and eight-pin connectors have been required to provide the additional power needed by the PCI Express card.

The ATX12V 1.0 standard no longer relied on the voltage regulator module, which was located next to the CPU. This supplied other supplementary voltages. Now the PSU itself delivered more varied voltages to be used within the different parts of the motherboard.

Later versions required even more power and so the ATX12V 2.0 connector (also known as 20+4) was a P1 connector with supplementary power supplied by the P4 connector, which clips on to the P1 connector.

The later ATX12V 2.1 standard uses six pins and provides 75 Watts of additional power. ATX12V 2.2 uses eight pins, and this was a variant on the six-pin design.

- **MicroATX:** It is worth mentioning that, although the connectors for the MicroATX and ATX power supply units are the same, the size of the unit itself is much smaller and so an ATX power supply will not fit into the chassis of a MicroATX system.
- **Dual voltage options:** Some power supply units have a **country selector** switch on the rear of the PSU, located next to the power switch and the mains cable. This can be either to 230 V for the UK, or 110 V for Europe/US. If this is set incorrectly (for example, 110 V when in the UK) then the PSU will receive too much power and will overload:



PSU voltage selector switch



# Video training

To summarize this section I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Computer Power Connectors (5:15):** <http://www.professormesser.com/free-a-plus-training/220-901/computer-power-connectors/>
- **Power Specifications (9:44):** <http://www.professormesser.com/free-a-plus-training/220-901/power-specifications/>



## **901.1.4 Given a scenario, select the appropriate components for a custom PC configuration to meet customer specifications or needs**

The A+ certification needs you to be able to support virtually any system but also to understand in general terms how a proprietary system such as a video editing workstation is not that different to a standard office PC. This section will look at some of the differences and nuances in tailored systems--what their requirements are from an end-user perspective, and what hardware or software changes are needed to support this requirement, culminating in the concept of Thick and Thin images, when considering our software management.



# Graphic/CAD/CAM design workstation

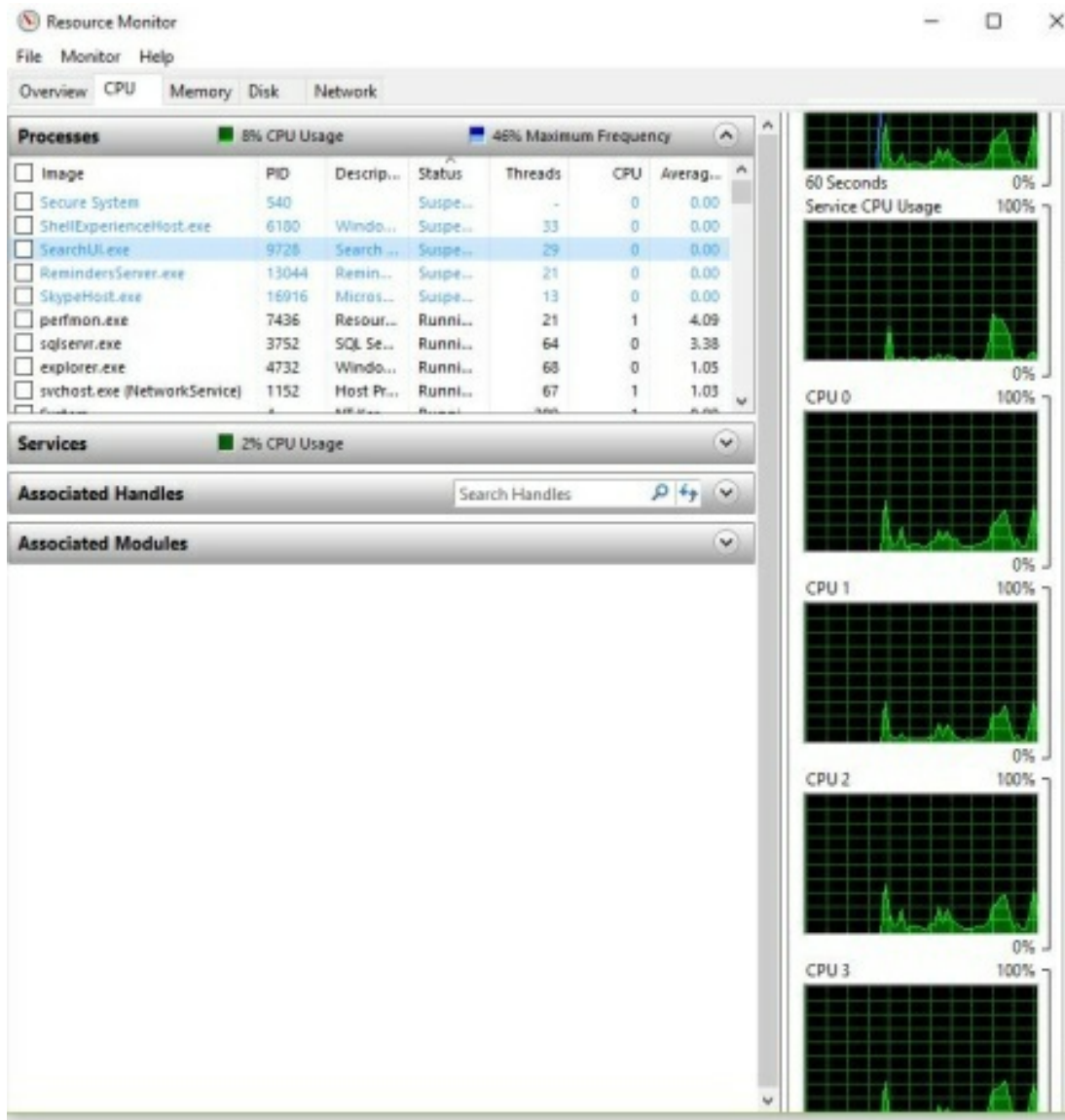
High-end graphics systems require the ability to render high-resolution graphics as quickly as possible. It is likely that the biggest requirement will therefore be a multicore processor with excellent, fast logic-processing capabilities. This load can also be shared by the Graphics Processing Unit--a dedicated chip found on high-end graphics adapter cards, taking some of the load from the CPU.





# Multicore processor

By splitting the calculations across several cores we can leverage parallel processing. The OS and application used must, however, support multicore processing:



Multicore processing at work



# High-end video

It is likely that the completed graphics may be an animation or, for example, post-production effects added to a digital film file. Here, rendering is across multiple frames with 24 frames per second as the standard framerate for film. For gaming this can go as high as 120 fps, or even higher.

The graphics card must be able to keep up--to render the images very quickly. Equally, the monitor must be able to display the images with a short refresh speed so that all of the images are displayed.

The two key metrics here are therefore the refresh rate and resolution.



# Maximum RAM

Graphics cards have a buffer cache and need to retain the images that have already been rendered in memory before they are released to other components, for example, to the monitor. As the rendered images may contain a variety of polygonal shapes within 3D space, there may be a lot of memory required before the eventual image can be rendered, rasterized, and sent to the monitor as just one frame:



Rasterizing 3D man



# Audio/video editing workstation

With a multimedia editing workstation edits need to take place in real time. This can be quite difficult to achieve without serious processing power. Dedicated systems such as Media 100 or SADiE use their own hard drive and processing banks, which work separately to the PC's processor - the PC acts like a monitoring tool and the data stays within the SADiE system. Most often, offline editing is worked on first--a **rough cut** is created and the edits are saved to a text-based log file. The media is then re-loaded into an online editor, the edits are imported from the log file and alterations made. The reason for this is the vast cost of hiring an online editing studio, so preliminary work can be done away from the editing studio, saving time.



eta-i.org is one provider offering an exam for Digital Video Editor.  
Certiport.com also cover Adobe Premiere exams and training.





# Specialized audio and video card

The audio and video card must not drop frames. That is essential. For this, the cards must be able to handle the data transfer speeds for high-definition resolutions and at large frame rates of at least 25 frames per second.



# Large fast hard drive

RAID 10 is an absolute must as this provides data transfer speed at block level while also providing fault tolerance. The physical drives themselves are typically solid-state, allowing for extremely fast data-access speeds.



# Dual monitors

By having dual or triple monitors, the editor can visually separate the preview window, the timeline, and the bin of storage materials. Simple drag and drop of material from the bin onto the timeline can make the process of editing video very easy. On the timeline, the media clip has a start and end point, and these can be changed by moving the drag handles to accommodate a new start and end point. Additional seconds of material are available but are not used--the exact frame specified as the in and out point are used by the editor.

When the editor is happy that additional resource material is no longer needed, unused top and tails for each clip can be purged (known as **trimming**).



# Virtualization workstation

With virtualization enabled in the BIOS, hardware system resources can be shared with the virtual PC. Moreover, Hyper-V allows one VM over another to prioritize system resources. System resources can be 'balanced' across the PC so that all VMs running can use the resources without any reduction in performance. Advanced Hyper-V virtualization systems such as Hyper-V Server supported by System Center can indeed turn on and off VMs, as they are needed and if resources are available.





# Maximum RAM and CPU cores

The key to virtualized PCs is how the resources are shared. Both cores and RAM can be shared; however, the more processing required the more intensively the resource is used, up to a point where the VMs and the host machine will all suffer a reduction in performance.

Some virtualized VMs such as a SQL database server require their own control of RAM and disk resources. It is therefore common to see a fully provisioned VHD hard drive file for SQL server to control.



# Gaming PC

A Gaming PC is a high-end PC with expensive and high-ability hardware such as a high-RAM graphics card capable of fast data rendering. The gamer is interested in quality and extremely fast feedback. For this reason the sound and vision are paramount.



# Multicore processor

Gaming is processor-heavy as has to render hundreds of polygon shapes comprising the overall image, every frame, every second. To do this it is common to see multicore CPUs, as the processor load is shared across the cores.



# High-end video/specialized GPU

To assist the processor, high-end cards with a large dedicated graphics RAM will render video instead of leaving this task to the CPU. This frees up CPU resources to focus on other processing.





# High-definition sound card

As a gamer, you want to be immersed into the experience, suspend your disbelief, and imagine that you are actually there. To this end, high-end stereo, and surround sound in particular, are used. For this, the audio card has its own processor capable of decoding audio and transmitting it to the speakers or sound bar. Typically, digital output is used (for example, HDMI, Optical, or RCA digital) to allow crystal-clear audio.



# High-end cooling

All of the above comes at a price. The power requirements are very high and with it a lot of fan noise and heat are generated. Thermal-pipe cooling and ultra-quiet fans are therefore commonplace.



# Home theatre PC

A home theater PC such as Media Server contains all of these--it is a dedicated box, a media file server, with encoding and decoding protocols loaded to support playback from a number of devices such as Blu-Ray and DVD. Modern home theater PCs are internet-ready, supporting Netflix, Amazon Fire, and other service providers who are supplying content in high-definition, digital formats.



# Surround sound audio

As digital stereo is required, it is common to see the home theater PC link through an optical connector, RCA, or HDMI to an amplifier capable of generating the separate audio channels supporting 5:1 Dolby surround sound.





# HDMI output

HDMI has become the most prevalent connection type supplying high-definition video and audio.



# HTPC compact form factor

Most home theaters are in fact dedicated devices--they are compact and made by a manufacturer supplying the device as part of a subscription package. A typical example of this would be a Sky Q decoder box, which is in fact a HTPC system.



# TV tuner

Less common are TV tuners. These typically were used to pick up UHF analog signals; however, the analog network has been turned off now within the UK and in fact this change has been rolled out globally now as we depend ever more on digital signals. The bandwidth has been now recycled to expand the radio, IT and mobile networks.

When we think about a digital TV tuner, we're referring to digital pickup via satellite or cable TV. The tuner is integrated into the set-top box, enabling connections to a variety of channels.



# Standard thick client

A **thick client image**, relative to a **thin image**, contains all of the software it is possible may be used within the company. While it may not be an exhaustive list and there may be licensing implications concerning running the same application on multiple PCs, the rollout of a thick image simplifies PC deployment as you have no need to customize the PC, or at least very little.

The disadvantage of the thick image is that it is quite bloated and therefore takes a long time to deploy the image.

The middle-way is a **hybrid image**, which is a thin image, partly configured with common apps shared across most, but not all, of the departments. It is used when the process of installing additional applications onto the thin image may actually take too long because different departmental requirements are diverse.

Of course, the other option is to create a series of thin images for different operating systems, different licenses, and different architectures, as well as different applications.





# Desktop applications

A thick client contains all of the applications needed across the environment. They are used on an as-and-when basis. The more pressing concern is licenses, given that the company may have purchased only a limited number of licenses **per computer and not per user**. If per user or domain wide then this is not a problem.



# Meets recommended requirements for selected OS

You have to be very careful to check that the software installed on the thick image works on all of the hardware systems it will be installed onto. For example, a 64-bit application will only work on a 64-bit hardware machine. Therefore, you cannot mix and match. You can add 32-bit applications onto a 64-bit image where the OS is also 64-bit only if it is tested to work on this setup, but then you run the risk that not all 64-bit hardware will support it.



# Thin client

A thin client is a PC's software image, standardized with only the generic common applications, roles, and features installed. In this way, we can efficiently distribute this common, generic image across the enterprise network and only have to install a few additional applications and configuration settings specific to the department the PC will be used by. The process of issuing the same image across the network to PCs that need it is referred to as deployment. This can be automated and, with the help of management-tier-level software such as Intune and System Center, the process can be automated - the network can effectively self-heal.

A friend of mine is the IT manager for a school of 350 PCs, approximately. She was firefighting regular, repeated problems week after week. As a solution, we implemented a common image that would work on all of the classroom PCs. If hit by a virus at the end of the week, we need not worry as all of the classroom PCs were re-imaged over the weekend, automatically leaving a clean and ready-to-use PC on Monday morning.

The process of deploying a thin image across a network of 100+ PCs may only take a few minutes, where by comparison, the process of installing from an empty box (a virgin PC) to the same software position may take one to two hours per PC.

A **vanilla image** is a PC that is at the point where the basic OS and rudimentary, common apps have been installed. The 'vanilla' typically has no unique security settings and will need to be SYSPREPPed to customize the security settings to uniquely identify the computer on the network, as well as to license the PC.

A **Gold image** or **Gold standard image** is one approved by the corporation to use. It has been rigorously tested for vulnerabilities.

System Center often starts rebuilding PCs with a thin image, then adds unique software and configurations specific to how the PC will be used.



# Basic applications

The thin image therefore contains applications common across the organization and ones which are centrally licensed for use by all staff. (for example, Adobe Acrobat Reader, Google Chrome)





# Meets minimum requirements for selected OS

A thin image is configured to meet the minimum hardware requirements - those of the lowest common denominator, so that the image can be applied to all machines. If required, a DISM command can be run to adapt the requirements for higher-specification machines, or a separate image is used for higher-spec machines.

At the time of writing, the minimum requirements for Windows 10 are as follows:

- **Processor:** 1 gigahertz (GHz) or faster
- **RAM:** 1 gigabyte (GB) (32-bit) or 2 GB (64-bit)
- **Free hard disk space:** 16 GB
- **Graphics card:** Microsoft DirectX nine graphics device with WDDM driver
- A Microsoft account and internet access



# Network connectivity

The process of receiving an image through deployment requires a network card. If set to boot from the NIC, the first stage is to acquire an IP address from a local DHCP server. Once the IP address has been received, a boot image is required. The Windows Deployment Server sends a boot image if the hardware lacks the support to load a complete image. The boot image contains additional hard disk drivers and network maps to obtain the full image.

Through deployment, it is possible to re-image several hundred PCs to a working state within a matter of minutes.



# Home server PC

A home server is often used as a file-share server or print server, to manage several file access points or printers across the home. It is designed to be left on and provides central access to resources.

The home server is generic in that it can be a media streaming server, a print server, or host a variety of other services used across the home network... bar one.

It is not common to find a common authentication server. That leads us into the realms of a proper domain network.



# Media streaming

One common use is to access media files from a file server. The data is not sent, but streamed to the presentation device. Devices that send a stream of data are referred to as media streaming devices. Most devices can stream with the correct software (for example, **Servillo**)





# File sharing

Files are shared across the network by the creation of a Universal Naming Convention path:

```
| \\<Computer Name>\<Shared Folder>
```

For example: \\Server01\MyShare

The share has its own permissions and the files/folder on the volume have separate security permissions (NTFS permissions). The permissions are cumulative with the most restrictive taking effect.

**Test question:** I have a share with read permissions. The NTFS permissions are set to Full Control. When I am accessing the shared folder across the network, what are the effective permissions? Answer: Read Ok, but what if I am physically sat at the PC and connect using File Explorer, accessing by volume letter and NOT by share?

**Answer:** As you are connected to and using the volume letter, the share is irrelevant. The only policy to apply is the NTFS security policy, so the answer is Full Control.

A file server is a common access point for files across the network.



# Print sharing

Although folders can be shared, so can printers--they are also objects on the network. The printer can be centrally shared but also managed from the print server.

There are three key security principles for printers:

- **Print documents:** This allows the user to print, or to cancel a print job they sent to the printer
- **Manage printers:** This allows the user to stop and restart the print device itself
- **Manage documents:** This allows the user to manage the print queue on the OS printer object



# Gigabit NIC

A Gigabit NIC has the bandwidth to support 1000+Mb/s, which is excellent for movie/High Definition file transfer, making it important for transfer from where the movie file is stored to where it will be presented.



# RAID array

A **Redundant Array of Inexpensive/Independent Disks (RAID)** is a collection of disks working as a group to give either/both fault tolerance or a performance boost:

- **RAID 0 (Striping)**: It refers to the fact that two or more disks are working as a group, sharing data sent out to the disk controller, sending a stripe of data to each disk in the group at the same time. Each stripe is different and forms the overall file. There are massive performance benefits.

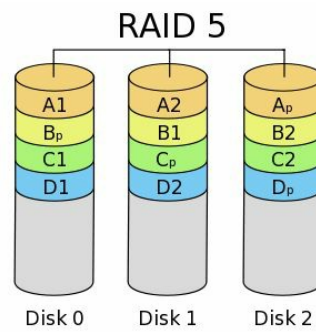


For an excellent example of this, look at Samsung SSD Awesomeness, which shows this principle across a group of 24 disks set as RAID 0: <https://youtu.be/96dWOEa4Djs>

- **RAID 1 (Mirroring)**: As an alternative, if you are more worried about physical redundancy, we can copy the same data to two drives. This does not give a performance benefit and the volume size is the same as one drive, but if one disk fails the other continues to provide the volume.
- **RAID 5**: (A variant of the earlier, now defunct RAID 3) means striping with parity. Three disks of equal size are used and the RAID 0 stripe is sent with data stripe A on the first disk and data stripe B on the second disk. The data saved is put through an algorithm, which stores a checksum based on the data in the two stripes, which is converted into a checksum. The checksum is a number derived by putting the data in the stripe set through a specific algorithm. It is not the answer to that algorithm and the process cannot be reverse-engineered. The checksum can only be reached if the stripes in both A and B are correct.

To repair a volume using RAID 5 you have to trigger the repair command, which may take several hours to complete. Each stripe is checked and the missing piece is eventually found. This differs from its predecessor, the now defunct RAID 3, in that the parity bit is cycled across the disks on every save:





- RAID 5 (striping with parity, cycled) The modern version of RAID 5 is RAID 6, which supports two disk failures within the volume. It needs a minimum of four disks and the parity bit is copied onto a further disk; yet again the party disk is cycled.



# Video training

To summarize this section I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Designing Custom Computer Systems (8:28):** <http://www.professormesser.com/free-a-plus-training/220-901/designing-custom-computer-systems-2/>



## **901.1.5 Compare and contrast types of display devices and their features**

There are a lot of different types of display on the market, each with their own use and purpose. We will look at some of the metrics used when discussing a display device, such as the physical media used (for example, Plasma screen versus OLED). We will look at display metrics such as the refresh rate, whether the data signal is analog or digital, and what this means when you use a generic port, which could supply either data type (as is the case with DVI), as well as the physical and rendered dimensions of the screen.



# LCD

The laptop screen is made up of a lightbox (a hollow cavity with a backlight to illuminate the translucent screen) and the screen. All modern laptop screens are LCD - Liquid Crystal Display. When electricity is applied to the liquid crystals, they illuminate as red, green, blue (or a combination of these adding up to white). The crystals overlap, forming a pixel. The power to the LCD array alone, however, does not make the information on the screen visible - the backlight provides further illumination.

Average screen sizes for modern laptops measured diagonally across the screen, not taking into account the frame surrounding the screen. Dimensions are as follows:

- **Ultraportable:** 13.3" or less
- **Thin and Light:** 14" to 16"
- **Desktop Replacement:** 17" to 19"
- **Luggables:** 20" and higher





# TN versus IPS

There are two types of laptop panel currently in use.

TN panels have very narrow viewing angles (if you look from the side across at the laptop screen you will see a distorted, or even inverse image), where the light image is shone directly out of the screen. These tend to be cheaper, and refresh rates (the speed taken to draw the complete image on the screen) are short. Screen color and brightness, however, is poor in comparison to IPS screens.

IPS panels are more expensive, with higher color and viewing angles but slower refresh rates. They are associated with use by graphics designers or architects, where high-quality detail is needed, but are not used by gamers or domestic users as the refresh rate is too slow.



# Fluorescent versus LED backlighting

This is typically a fluorescent (Cold Cathode Fluorescent Lamp or CCFL) light strip within the 'lightbox' area to allow the user to see the information on the screen.

AC power is used to illuminate the backlight. However, where is this AC (mains) power coming from when a laptop is a mobile device, not connected to the mains? The laptop is powered by a power supply, which steps-down the voltage and changes its nature from AC to DC. A low-power DC voltage is applied to the laptop battery, which recharges but also conditions the incoming power, where it is then used by the laptop components.

The fluorescent light within the backbox requires AC, not DC, to function, so the process is reversed at this point. An inverter is a circuit board that is capable of creating AC power from DC, which in turn powers the fluorescent light.

In order to manage brightness, PWM (pulse width modulation) is used. The backlight is on for a certain period of time and off for a certain period of time. The light is effectively strobing. When you adjust the brightness setting you are altering the length of time the light is on and off. The earlier version, CCFL, does not react as quickly as LED to state change, producing a fading on the screen for a short time. LED does not do this.

Test this with your own laptop by switching the monitor off, then back on. On laptops, use Alt+ Tab to switch between a full-screen black image and another app that is white, and you will see that it takes a short time for the full brightness to be reached.



# Plasma

An older system but occasionally still used, a plasma display contains cells of non-combustible gas and mercury. With power, **ultraviolet (UV)** light is created providing a good image display and fast refresh times.

LCD advancements and their relative cost have meant that plasma is less common now.



# Projector

LCD and LED projectors project the image onto a screen or wall. The image is therefore much larger than one possible from a screen. The problem with LCD is that it relies on a high-watt bulb, which produce a great deal of heat and are prone to burn out periodically. Any movement will typically also cause the bulb to fail.

LED uses light-emitting diodes, so there is no bulb to replace. An LED unit can last for several hundred hours, but are typically more costly.

Let the projector completely cool down before moving the device. The power off function actually triggers the fan speed to increase to expel the hot air and to attempt to reduce the lamp's temperature before final closedown.





# OLED

Organic LED does not require a separate backlight--as the OLED is powered it also generates luminescence, not just color. Contrast and colors are much better from OLED in comparison with LED. OLED devices are thin and highly portable.



# Refresh/frame rates

The frame rate is a measure of the number of images (frames) displayed per second. For internet animation this number is typically 12 fps. For film it is 24 fps. For UK PAL TV it is 25 fps.

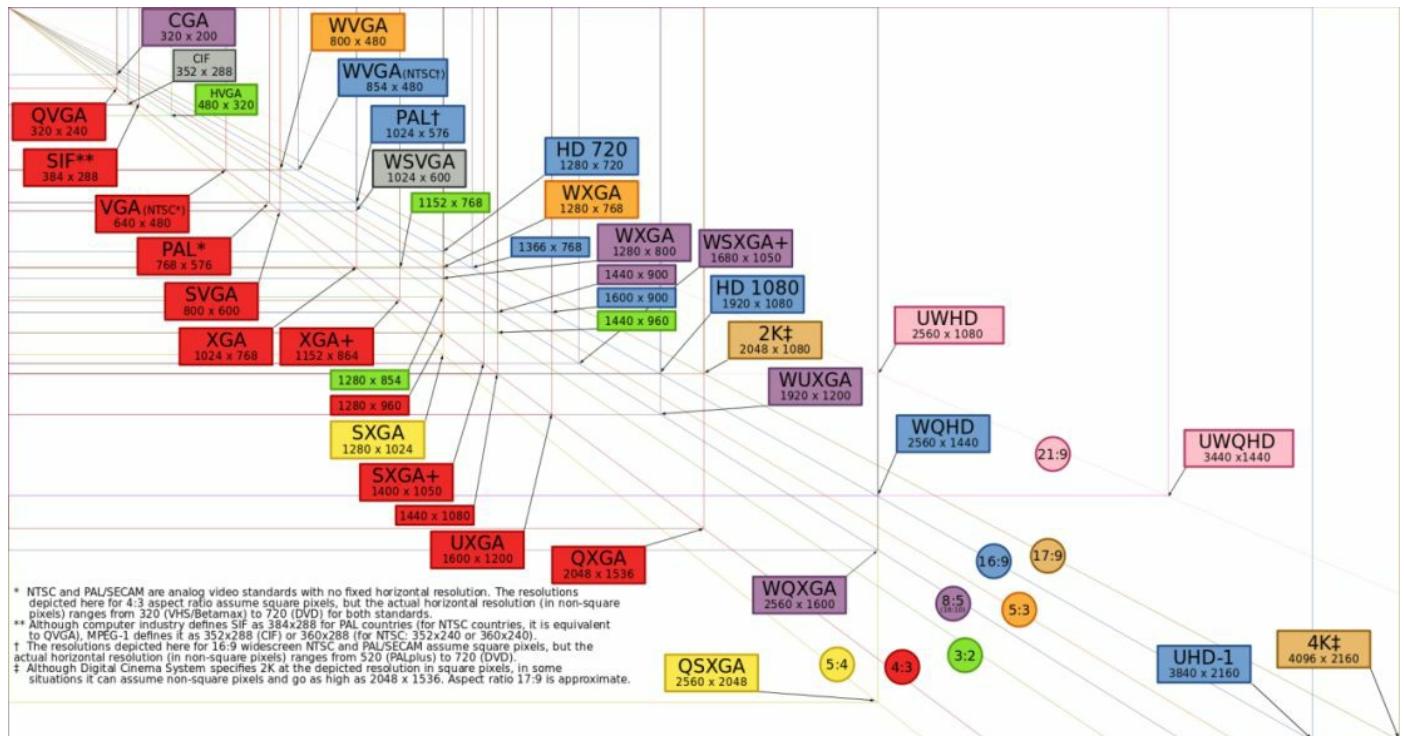
The refresh rate is the amount of time between drawing each frame. You want this number to be as small as possible in order for the frame rate to be achieved.

To a media editor, the term framerate is more important as it denotes the quality of the overall experience. To a technician, we are concerned with refresh time. Both are measured in Hertz.



# Resolution

Resolution refers to the number of pixels that can be drawn to make up the image. They are defined by an aspect ratio--the ratio of width:height:



Video resolution standards



# Native resolution

Monitors are designed with a standard resolution they are intended to be used for. They support some adapted resolutions, but from this base point. The pixels might not match up exactly and as a result some distortion might occur.





# Brightness/lumens

Lumens are a measure of light provided by the screen. Three thousand lumens would be the lightness of a monitor visible within a dark room. Six thousand lumens is a visible monitor in a lit room.

Brightness refers to the luminance of the display. This can be adjusted by the user to suit. The brightness is measured by candela per square meter.

Do not confuse brightness with black and white balancing. The monitor can be calibrated to know that the darkest possible pixel is black and the brightest is white. The contrast ratio is the measure of difference between these two values.

Every monitor and graphics card is different and it is necessary to calibrate the two so that the image is provided by the PC correctly and interpreted by the monitor correctly. To help with this, the graphics card and monitor drivers contain calibration data to ensure that any work done will be consistent if moved to another PC with different hardware.



# Analog versus digital

As described previously, analog refers to the intensity of a signal over time. It will graduate and each different level is represented by a number against time. The signal is continuous but the number will change.

A digital signal represents the presence of a signal against time. What is sent is a sine wave, and we are checking for the presence of a signal at a point in time and representing this as 1 and 0, so the strength of the signal is not relevant.

DVI can support analog or digital. HDMI is digital only.



# Privacy/anti-glare filters

A privacy filter is a polarizing filter placed over the screen. Light beams are only allowed through to the user looking directly at the screen. The filter is used to stop shoulder surfing (a person standing nearby from glancing across at your screen and reading any sensitive data which might be on there).

Anti-glare filters also work by limiting the light splay so that fluorescent lights do not cause a glare across the screen.



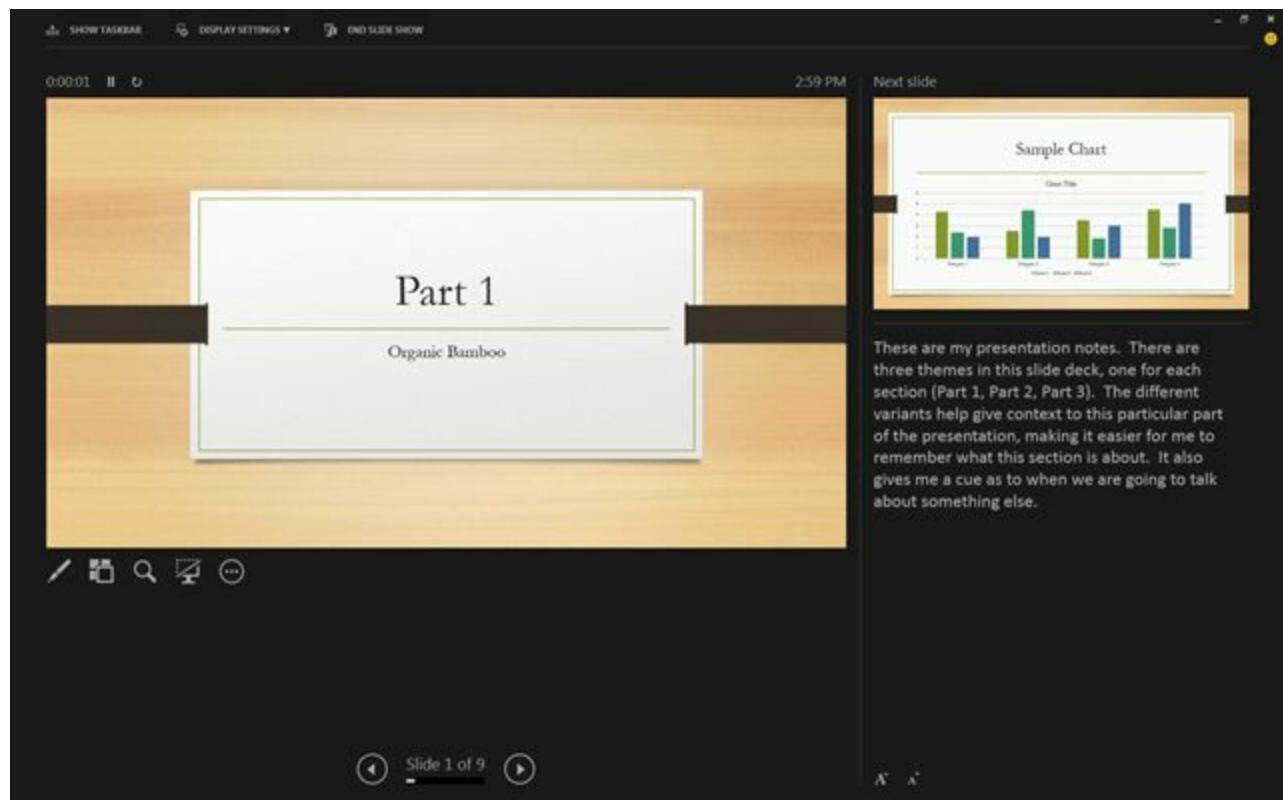
# Multiple displays

As described previously, multiple displays can enable the user to increase productivity by extending the user environment's footprint. Video editors often use three screens--a **bin**, an **editor**, and a **preview**. This saves time where otherwise you would have to switch from one application window to another.

Apple systems were always built with this in mind--forms and app windows are floating but can be docked (pinned to a part of the screen). In this way the app could span multiple windows, with lesser-used plugins and widgets moved to a separate physical space.

As an IT trainer I teach a lot of Microsoft courses. Here, instructions are supplied using a PDF file. The labs are typically online, so accessed through a web browser. By putting the instructions onto one screen and the lab on the second screen the user's experience is increased as they are not having to take their eyes away from the browser view window but can concentrate on the matter in hand.

By setting the second screen to mirrored, where the second screen is in fact a projector, you will be able to project the same information as you can see on your presentation laptop. Microsoft Office 2013 now enhances this by providing a second screen option where you can read your presentation notes and see a view of the current and next slides, while the second screen (the projector) presents your slide in full.



PowerPoint 2013 presenter view





# Aspect ratios

Pre-2006, the most common display format was 4:3, which is the older terrestrial TV standard. We now use 16:10, as the majority of media consumed is film. Both 16:9 and 16:10 are common for widescreen formats, and widescreen laptops are now commonplace.

The aspect ratio is the ratio of width to height:

- **16:9:** 16:9 is the standard for non-HD television. It is the international format for HDTV and is supported by the DVD standard.
- **16:10:** Where 4:3 and 16:9 are based on TV and film, 16:10 is a PC format. It supports the following resolutions:
  - 1280×800
  - 1440×900
  - 1680×1050
  - 1920×1200
  - 2560×1600



Of the two, 16:9 is by far the more popular; however, Android devices use 16:10.

- **4:3:** Originally the ratio used in 35 mm film and later with terrestrial TV.



# Video training

To summarize this section I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **An Overview of Display Devices (6:21):** <http://www.professormesser.com/free-a-plus-training/220-901/an-overview-of-display-devices/>
- **Display Specifications (6:17):** <http://www.professormesser.com/free-a-plus-training/220-901/display-specifications-2/>



## **901.1.6 Identify common PC connector types and associated cables**

This section covers all of the non-network connector ports. The majority of this section looks at the different display connectors - what they look like and where they may be used. We then extend into display cables and consider the signal sent on each cable type - is it digital? Is it analog? Is the video signal sent on one cable or split into the three primary colors--red, green, and blue?

We then consider other types of cable used for data transmission, such as eSATA, USB, and Firewire. We consider cable length and the speed of data transmission.

Given the variety of devices and connectors on the market there will be times when we need to convert from one type to another. We end this section by looking at a variety of adapters and converter cables capable of adapting the signal and extending functionality, crossing the Apple/PC divide, or providing legacy compatibility for older hardware.



# Display connector types

Earlier in [Chapter 1](#), Hardware 1.1 (901.1), we looked at the physical port. Here I want to contextualise where each type of DVI connector is used and how to determine when to use them.

- **DVI-D:** DVI is a common standard associated with Apple, as well as generic PCs. DVI-D refers to a digital signal sent across the cable.
- **DVI-I:** DVI-I (Integrated) is a composite port, which is capable of supporting either digital or analog.
- **DVI-A:** DVI-A is an analog signal.

Refer to the DVI image earlier on in the chapter.

- **DisplayPort:** DisplayPort was developed by the **Video Electronics Standards Association (VESA)**. It was originally designed to carry video from the PC to a monitor, but is capable of also sending audio and for file transfer. It was designed to replace VGA and DVI as a common standard. It is possible to make DisplayPort backward compatible with VGA and DVI.

DisplayPort uses its own proprietary protocol capable of sending display packets, similar to internet packets. Video supports 16 bits per color channel and audio supports up to eight channels of 24-bit 192 KHz, so would be perfect for home theaters and surround sound.

DisplayPort is, however, not compatible with HDMI.

- **RCA:** The RCA photo adapter is a single wire with a male pin and earth sleeve. Typically, three are used to provide audio and video. (Yellow for composite video, white for stereo channel A and red for stereo channel B.)

The RCA signal is analog and the cable is considered to be **unbalanced**, as the ground voltages of the end equipment are not matched. As a result of this, the cable will pick up interference as data travels along it.

RCA is commonly found in home systems and the audio ports can be combined into a 3.5 mm mini-jack plug to connect to domestic devices such as a Wi-Fi:





Composite ports

- **HD15 (for example, DE15 or DB15):** The RSA standard DE 15 refers to what is more commonly known as the VGA port (to be technically accurate, original VGA is a 12-pin plug whereas SVGA is 15-pin). It is an analog signal of red, green, and blue channel pixel data. No sound is transmitted along the cable:



High Density, 15-pin (HD15) male connector

DB15 is the earlier 2-row equivalent. This was used to connect MIDI devices into the sound card:



DB15 male connector

- **BNC: Bayonet Neill-Concelman (BNC)**, also known as **British Naval Connector** is used with coaxial cable. It is a simple connector with a locking ring, capable of holding the cable in position. A later variant is the F-connector (with a hexagonal nut to screw the cable into position). It is famous for use with audio and radio transmitting equipment, and latterly with networking, especially in the creation of token-ring networks, as the cable is reliable, sturdy, and easy to use.
- **miniHDMI:** As explained previously, **High-Definition Multimedia Interface**

(**HDMI**) can transmit audio and video in digital form. Type-C was a smaller connector designed to fit to camcorders in order to transfer data directly from the camcorder's playback to be digitized on the PC.

HDMI-C's connector is 10.42 mm x 2.42 mm and uses the same 19-pin standard as earlier HDMI.

- **miniDin-6:** Another common cable now sadly not used is the DIN plug. Created by the Deutsche Institut fur Normung (The German Institute for Standardization), it was the USB of its day used to connect home amplifiers with cassette and reel-to-reel recorders. A PC variant of this was in fact the first PS/2 port used in early IBM systems to connect the keyboard to the PC. The smaller micro PS/2 used today is based on this early cable.

Typically, the purple miniDin is used to connect a keyboard and the green miniDin is for the mouse. The keyboard controller chip is backward compatible to support the mouse as well:



miniDin connectors



# Display cable types

This section will focus on common display cable types:

- **HDMI:** HDMI is a common digital format used to connect the graphics card or set-top box to a TV. It sends a high-quality video and audio signal.
- **DVI:** DVI is an interchangeable format. Depending on the connector and cabling, the DVI cable can send video and audio. The DVI signal can be analog or digital, again defined by the pinouts on the connector. The interchangeable format is used in situations where a monitor can support either signal, and it depends which device the cable is connected to.
- **VGA:** VGA is an analog signal comprising of three primary color channels. The signal sent is analog. No audio is sent.
- **Component:** Here, the red, green, and blue channels are split onto different cables. Component requires separate cabling for audio--only the video signal is sent.

Typically, the early component signal is analog; however, modern home theater systems send a digital component signal.

It has been replaced by DisplayPort, or DVI:



Component video cable with stereo RCA audio

- **Composite:** The composite signal is, in fact, a combined analog signal. The Red, Green, and Blue channels have been merged and are sent using a standard TV transmission at 480 interlaced, or 576 interlaced resolution. Composite is synonymous with TV broadcasting and can often be found as a connection for the Nintendo Wii, DVD recorders, and other devices where resolution is not a major concern.
- **Coaxial:** Coaxial is commonly associated with connecting the satellite dish or cable TV source to the decoder box. The decoder box is, on modern systems, effectively a home theater system. The signal can be run for long lengths and the

protective wire braiding (shielding) protects the signal transmitted through the core copper wire from crosstalk and other interference. Coaxial would typically terminate with a BNC or F-connector:



F connector on coaxial cable



# Device cables and connectors

In the laster chapter we focussed on video and output connectors. This next section will consider data connectors.





# SATA

Serial ATA cables are typically up to one meter in length. The data cable has an L-shaped connector and is therefore keyed. The cable is sturdy and is used to connect the SATA adapter to the hard drive.

Note that the SATA power connector is an adapted Molex. It really only needs 3.3 V; however, modern SATA devices do support and regulate down the power from 5 V to 3.3 V.



# eSATA

External SATA supports devices located two meters away from the eSATA port, located at the rear of the PC. You will notice that the eSATA cable is keyed and has a locking clip, but the port is not L-shaped:



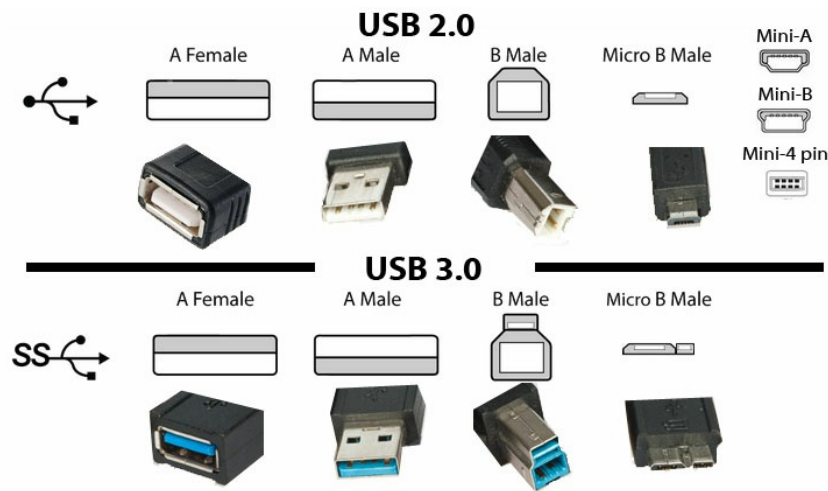
eSATA cable



# USB

The Universal Serial Bus is a common adapter. USB A is keyed with a base plate denoting the bottom section of the port. USB B (device end) is keyed ending with a square connector with chamfered top edges. USB supports up to 127 devices on one cable.

USB version three typically has a blue base plate to denote its speed:



USB 2 and 3 ports



# Firewire (IEEE1394)

Firewire is typically 4, 6, or 9-pin. It supports up to 63 devices on one cable:



**USB 2.0**  
B-plug  
480 Mbit/s



**USB 3.0**  
B-plug  
5 Gbit/s



**FW 400**  
4-pin  
400 Mbit/s



**FW 400**  
6-pin  
400 Mbit/s



**FW 800**  
9-pin  
800 Mbit/s



**Thunderbolt**  
Copper MDP  
10 Gbit/s

USB versus Firewire and Thunderbolt ports





# Audio

As discussed above, audio can be carried by the following:

- HDMI
- DVI
- Thunderbolt
- RCA
- Composite



# Adapters and converters

So far we have considered pure connectors only, however the signal can be adapted to fit across another connection medium. This section will look at common-use connectors, but always be careful when combining analogue and digital connectors.



# DVI to HDMI

A DVI to HDMI adapter is a simple dongle enabling the digital DVI signal to be sent into an HDMI port. Please note that the signal has to be digital for this to work. It is possible, but more expensive, to buy a DVI adapter box. This is in reality a media converter, which will perform an analog-to-digital conversion, generating the digital signal.

Usually, you only require the adapter dongle as your sending signal is digital:



DVI to HDMI adapter



# USB A to USB B

USB type A to USB B is a standard cable connecting a PC (A) to the USB device (B):



USB A to B cable





# USB to ethernet

Some MacBooks and laptops, for reasons of size, do not have an ethernet card fitted as standard. As USB has overtaken PCIExpress, this functionality can be offered with a USB to ethernet card:



USB to ethernet cable



# DVI to VGA

Some monitor manufacturers use DVI-A as a standard to replace VGA. DVI is commonly found across Apple devices, where it appeared later on for PC users. The integrated video card housed on the motherboard is typically VGA, and separate graphics cards would usually have one VGA port and one DVI port. If you are using two monitors of the same make and model, and require dual-screen capability and want to use both ports on the graphics card, you will need to convert the second port. As the analog signal does not need any conversion, DVI to VGA dongles are extremely cheap and easy to come by:



**NB:** This will only work with DVI-A. The trick is to ensure that you connect the correct way around. DVI to VGA dongles are available to convert and connect both to and from VGA.



DVI to VGA adapter



# Thunderbolt to DVI

For Apple users, Thunderbolt (in reality we are describing Mini-DisplayPort) can be converted to DVI. This is a digital signal:



Thunderbolt (mini-DisplayPort) to DVI adapter



# PS/2 to USB

As both are serial linkages, it is possible to connect a PS/2 device, such as a keyboard to USB:



PS2 (miniDIN) to USB converter





# HDMI to VGA

Although HDMI is a digital replacement for analog video standards, it is backward compatible with VGA:



HDMI to VGA cable



# Video training

To summarize this section I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Display Connectors and Cables (9:01):** <http://www.professormesser.com/free-a-plus-training/220-901/display-connectors-and-cables-2/>
- **Device Connectors and Cables (6:26):** <http://www.professormesser.com/free-a-plus-training/220-901/device-connectors-and-cables-2/>
- **Adapters and Converters (6:28):** <http://www.professormesser.com/free-a-plus-training/220-901/adapters-and-converters/>



## **901.1.7 Install and configure common peripheral devices**

Installation really only forms a very small part of this section, as most of the devices considered in this section will work 'out of the box' with generic drivers. These 'plug and play' devices are designed to be physically plugged in while the system is running. The OS will then automatically install them with little additional effort needed. (Some devices may require video drivers, or calibration.)

The section is broken into input devices, output devices, then finally devices that are both input and output.



# Mouse

It is very easy to install a mouse. PS/2 mice are connected to the green PS/2 port on the motherboard. USB mice are connected at an available USB port. The Operating System contains generic drivers for common mice, so although it is recommended to update the drivers, the mouse will work 'out of the box'.





# Keyboard

The POST test will check to see if a keyboard is installed. As with a mouse these could be either PS/2 or USB. I would advise against the use of wireless keyboards when attempting to install the OS as these require the presence of a working Operating System before the drivers start to work. The USB and PS/2 keyboards conversely are supported by the bare-bones system, allowing you to trigger escape sequences to access the BIOS configuration menu, advanced startup menu, or to perform a factory restore using a hidden partition.

The keyboard, as well as having generic drivers, requires specific drivers to access additional buttons and media functionality. The codepage set within the Language area of the Operating System determines which keys correspond to which symbols. If this is not set matching the type of keyboard you have then you will get incorrect symbols as opposed to key presses.

For example, I often run Microsoft labs. The virtual machine is set to US keyboard settings, so the @, ", #, and ' do not match my keyboard. This can easily be fixed by altering the keyboard and language settings in the virtual machine (or learning the differences and making do).



# Scanner

Scanners are devices able to take a digitized image of a document. They are often used by businesses to archive or store a letter or form in electronic format. Document-archiving companies can batch process thousands of documents, encode them, and store them onto disk or onto a network share.

The scanner requires an application to control the scanner itself and a TWAIN driver to be able to convert the data into a format the PC can use:



A flatbed scanner



# Barcode reader

A barcode reader is a USB device sending serial data in the form of an ISBN of barcode. The thickness of the lines is converted into a code sequence and this code is then passed into the application, which then stores this number sequence as part of a database record. The reader requires a specialized driver be installed prior to first use:



Barcode reader



# Biometric devices

As with the barcode scanner, the OS driver has to be installed before the hardware is connected. Biometric devices install an authentication certificate onto the OS, which can be used to replace, or alongside, the username and password, forming a second factor. A typical biometric device found on enterprise laptops is a fingerprint reader.





# Game pads

A game pad typically connects through a MIDI or USB port. Again, the hardware driver has to be installed. These pads allow for quickfire movements associated with gameplay. On games consoles, the driver is already installed and is part of the OS:



XBox 360 gamepad



# Joysticks

Where the gamepad allows for quick control using a series of buttons to simulate moving an avatar, jump, run, crouch, fire, block, and to access the game menu, the joystick has a simpler function--it allows movement of the game avatar in the compass directions, with two further buttons to fire weaponry (action buttons).

The joystick is modeled on the design of a control stick as used in fighter jet engines and is synonymous with flight and racing games.

Most joysticks now connect with USB, although MIDI joysticks can still be found:



Joystick

An interesting aside is the Nintendo Wii, which fitted a gyroscope and wireless connectivity into their control stick, combining the joystick with a gamepad. This has been extremely popular for the younger and more inexperienced gamer, opening up gaming to the family:



Wii controller with safety wrist strap



# Digitizer

If you need to draw your signature or trace the outline of a shape, a graphics pen or digitizer is for you. As with a scanner, the device requires the driver to be installed first and has proprietary software linking it to more well-known applications. Digitizer pads are often used by graphic designers in order to capture fine detail and to draw with more precision than is possible with a mouse.

Advanced digitizer tablets actually show the screen's output onto the draw surface. With the advent of Microsoft Surface, massive integrated PCs designed with architects and graphics designers in mind, these small pads are not as commonly used as they once were:



A digitizer tablet



# Motion sensor

A part of CCTV security web cameras and motion sensors can be placed across a building and send data to a security PC, which will then typically record video footage as evidence, or trigger an alarm.





# Touchpad

As a variant to this, the touchpad uses the mouse driver and is able to provide the same functionality as a mouse. Touchpads are common on laptops. If required, the touchpad can be disabled as for some people it gets in the way and if you prefer to use a mouse anyway it can be a little annoying. However, if you are mobile then the touchpad is an essential replacement for a mouse:



A laptop touchpad



# Smart card readers

Following on from the fingerprint reader, some enterprise keyboards have an ID-card reader (referred to as a CAC Card Reader), which reads the authentication information stored on the ID card's chip:



Keyboard with CAC card reader



# Digital cameras

A digital camera is designed to take photos when mobile and away from the PC. Typical PCs will have a media bay where the SD storage card can be loaded and the saved files transferred onto the PC for further editing or archiving:



Digital camera



# Microphone

USB or 3.5mm-jack microphones rely on the audio card drivers and editing software to be able to then record an audio file (for example, Sound Forge or Audacity). Modern laptops and phones have a microphone embedded into the hardware, which is supported by the OS.





# Webcam

As with the microphone, modern smartphones and laptops have a webcam mounted on the top of the display. This is only enabled when triggered for use by an application (for example, WhatsApp on the Android Smartphone, or Skype on the PC):



Microphone and webcam on top of laptop screen



# Camcorder

As the digital camera, the device is intended to be used away from the PC and for the storage to be uploaded separately. Modern camcorders can store onto external storage, although early models store to tape, at which point an analog-to-digital conversion of the recording has to be performed and the material resaved as a movie file onto the PC.



# Output devices

This section will now focus on devices which deal with output other than that covered by the monitor section earlier.



# Printers

Technically speaking, the hardware (the machine that prints out paper) is referred to as a print device. The printer is the print object located in the Printers and Faxes menu.

A LaserJet printer uses ionized carbon and wax (referred to as toner), which is coated onto a photosensitive drum. Static charge is used to attract toner from the drum onto the paper, at which point the sheet of paper passes over a heated roller, which warms the toner, which then dries and sticks to the paper.

The laser printer's drum covers one third of an A4 sheet. Three turns of the drum complete the image for one sheet of A4.

Conversely, an inkjet prints one line at a time.





# Speakers

Speakers typically connect through the RCA or 3.5mm mini-jack ports on the audio card, although USB speakers are also common. The speaker is a cone with an electromagnet at its base, which vibrates, generating a sound we can hear with the human ear.



# Display devices

The display device is a screen that provides a visual display. We use this to watch video, surf the internet, and interact with the PC's environment. There are many different resolutions, a large number of which we covered earlier in this chapter.



# Input and output devices

Some devices provide output but can also accept input. These are covered in this section.



# Touch screen

A touch screen allows the user to interact by pressing onto the surface of the screen. The point at which the user presses is recorded and this is converted into a mouse action for this point.

If the user moves their finger across the screen this is recorded as a gesture. Different gestures are possible based on one or more touch points. For example, if you are to use two fingers and then move the fingers away from each other this would indicate that the user wants to zoom in.

Touch-enabled devices also include book readers, tablets, smartphones, and even ATM cash machines.

Touch can be **resistive** or **capacitive**. Capacitive touch uses the fact that the body has a certain electric charge and that something other than air is surrounding the point on the screen. It is accurate and does not require a special stylus. Resistive technology is somewhat older. Behind the screen lies a grid and the user has to press onto the screen, creating the recorded point.

Both technologies need to be calibrated regularly. Here, in test mode, a series of key points on the screen are pressed by the user and these are used to ensure that the device is accurately responding to presses.





# KVM (Keyboard, Video and Mouse)

It is common in server rooms and small offices to see, where there is a limitation on space, one keyboard, video monitor, and mouse attached to two PC cases. Here, the KVM can control two active PCs at the same point in time, but reducing the hardware required to do so. A special key combination is used to switch between the two wired systems.

In a server room, it is common to find approximately 10 blade servers in a rack with a 'workspace' in the center of the rack. This is a designated area set at a height so that the administrator can use this area as a desk and control the servers from here. The area contains a monitor but also a mouse and keyboard on a shelf that pulls forward. The KVM hardware is wired through a KVM box to each of the servers, and a key combination can be used to swap control from one server to another.

If you instead use third-party remoting software such as Teamviewer to connect to a series of servers that are rack-mounted, only one of the servers at any one time will be deemed to have a physical connection to the monitor. The other graphics cards, even though they are wired into the KVM, are effectively 'disconnected' because the electrical circuit is only live to the server in use. Teamviewer will be able to authenticate and start a session but will receive no output:



A KVM switch



# Smart TV

Most modern TVs have built-in firmware allowing for internet access and access to a variety of other devices and systems. For example, the TV on its own may be able to connect to the internet and be used as a rudimentary computer; however, no hard drive is present. Smart TVs allow for access via USB, so a USB flash drive could be used as a file store. USB and Wi-Fi are both common to connect to a keyboard, and the remote control typically can also move a pointer on the screen or navigate the built-in menu system.

More recently, Kodi and Amazon Fire have become available, which are purchasable USB drives with special OS software that connects the TV to a media server. By signing up to such a subscription service you can obtain access to new content otherwise not available or available only through a cable TV or satellite provider:



Samsung Smart TV menu



# Set-top Box

Even smart TVs cannot decode proprietary encoded signals, so separate to the smart TV, or even on an older non-smart TV, a set-top box was needed to decode the incoming signal from the satellite provider or cable TV company.

The encoding was usually also tied to your subscription account, so management information could be sent to the box to downgrade/upgrade the box remotely:



Sky Q box with remote



# MIDI-enabled devices

The **Musical Instrument Digital Interface (MIDI)** was an offshoot of development into audio cards and was in fact one of the most significant developments for IT in the 1980s. The MIDI port was a D-base (shaped) 15-pin port used to connect external devices capable of sending an input signal. This typically was the connection used to connect a synthesizer or electrical drumkit to the PC, but in later years was used to control the pitch, timing, and triggering of music samples:



Pianist using a synthesiser to send MIDI data

More recently, MIDI (which is really just a communications protocol) can be sent using a USB to MIDI dongle - it does not have to be through a dedicated sound card.

Any sounds generated by the sound card use waveform samples, which are then pitch-bent to match the MIDI data. MIDI is a specific key press and the length of time it was pressed for, against time.

The MIDI port on the sound card can also be used by gamers to connect a joystick, or other external adapter (for example, a racing car steering wheel) and was in use long before the wireless capability presented by the Nintendo Wii.



For more information about how MIDI can be used to create music, check out this excellent video at Propellerhead Reason's website: <https://www.propellerheads.se/en/reason/creative-flow>





# Video training

To summarize this section I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **An Overview of PC Input Devices (7:40):** <http://www.professormesser.com/free-a-plus-training/220-901/an-overview-of-pc-input-devices-2/>
- **An Overview of PC Output Devices (1:48):** <http://www.professormesser.com/free-a-plus-training/220-901/an-overview-of-pc-output-devices-comptia-a-220-901-1-12/>
- **An Overview of Input and Output Devices (2:57):** <http://www.professormesser.com/free-a-plus-training/220-901/an-overview-of-input-and-output-devices/>



# Summary

This chapter covered a wider section of hardware components extending out from the motherboard to the wider external peripherals. We also considered more than calculations performed by the PC but how the PC will interact with us.



# Hardware 1.3 (901.1)

Okay, so we are through the thick of it. The hardware module is a massive amount of learning at three book chapters long, but it is worth it. This final section is going to keep our focus with imaging and interaction on the periphery of the PC by focusing on document imaging and scanning--that is, input and output to external documents and sources. We are going to focus on printers and scanners, SOHO operations and how to communicate to such devices.

The main focus for you is to learn exactly how a laser printer works. This is absolutely crucial and I trust that I have explained it well enough.



# 901.1.1 Installing SOHO multifunction device/printers and configure appropriate settings

In this chapter, we focus on the home user or small office. Sticking with the concept of a device that is both input and output, we consider two-way communication (duplex) and where this may be used. We are really leading up to a large discussion later on in the book on print devices and how they work, but at the moment introducing the concept that a peripheral device can talk back to the PC, reporting status data or requesting more data.

Some devices are physically connected to one PC. In order to share this device, the PC has to act as a manager and process any share requests (for example, I would have to set up a print server). However, modern wireless devices in particular (for example, SOHO wireless printers) can accept print jobs from multiple devices. We look at some of the wired cabling used, then explain the wireless protocols that are so important to modern communication.

We then take the analogy further by considering printing from the cloud--an internet storage facility which can now also send print management commands to any computer it is managed to communicate with, anywhere on the planet. Geography is no longer a problem.

This takes us to other uses of wireless and sharing such as AirPrint or the Bonjour service (where devices in the neighborhood broadcast a hello packet and can be discovered as a new device by your OS.)

Considering the fact that we are telling people around the device that there is a device present, this can lead to data privacy issues--what if the print stream were intercepted by someone nearby? What if a file were stored in the cache on a hard drive and although the file was deleted, somebody else logs in and manages to retrieve the document from the temporary (cache) file? This leads us to consider a major concept covered in the Network+ and Security+ exams, also referred to in [Chapter 9](#), Security (902.3).







# Using appropriate drivers for a given OS

This next section will look not only at the concept of a driver and how it can be used to send basic data to external periphery such as printing a document, but also additional configurations you may wish to set which are attributed to the driver, such as whether or not the printer is capable of duplexing.



# Configuration settings

The key factor here is the architecture of the OS--the driver file should be the same as the architecture of the OS installed. For example, if you have 64-bit hardware you should install the 64-bit version of the OS and the 64-bit version of the driver.

It is important to note that the 64-bit system is backward compatible and can support 32-bit drivers as well, but ideally you need to be installing the same architecture of driver as the OS can support.

For servers in particular, drivers should be digitally signed, meaning there is an additional certificate file attached to the driver to provide information to the OS that the driver has been tested by the OS vendor and is trusted to operate on this OS.

For printer and scanner drivers, install the driver first and then attach the device (unless the instructions with the device say otherwise). This differs from most other plug-and-play devices, which require the device to be added first; then the USB port is linked to the device, the ID chip on the device is read, and the appropriate driver selected if it exists as part of a local driver store.

Always ensure that you have the latest drivers from the manufacturer. Avoid third-party driver sites as these often have virus-ridden files.



Did you know that TWAIN (as in a TWAIN scanner driver) stands for **Thing Without An Interesting Name?!?!?**



# Duplex

In relation to print devices duplex refers to double-sided printing. Advanced print devices are capable of re-feeding the paper back through the mechanism to print the reverse side.

The term, however, is ambiguous, as the term duplex also refers to two-way communication and the use of the data bandwidth. Here we tend to say **data duplexing**.

But how does data duplexing work? Modern printers, as well as sending data to the print device, also retrieve management information about the print job, such as the status through the print of the page or any error messages, which can then cause the job to pause until the error is cleared.





# Collate

With larger print devices such as photocopiers it is common to see a **collator**. This is a series of trays--each page in a print run is printed out and stored on a separate tray in the collator, starting with the first page. If the print run is for 10 copies of a document that is five pages long, then all 10 copies of page 1 are printed first. If we are duplexing, then page 2 is printed on the back and the first completed page is sent to the collator. One copy of this first double-sided page is stored with one sheet per tray.

The print device then moves on to sheet 2 (pages 3 and 4) and again one copy is dropped into each tray.

The print device then prints sheet 3 (page 5) and one copy of dropped onto each tray.

The trays in use now have the completed document in each of the 10 trays used. If the document needs to be stapled (professionally, this is referred to as **stitching**), the collator is also capable of this:



A print device collator



# Orientation

Orientation refers to the direction in which the text is printed onto the page. Orientation may be portrait (thin width, long length), or landscape (long width, thin length).

When printing double-sided it is important to know which side of the paper will be printed on and which way round the print will be printed (for example, which is the top of the sheet). This will differ on different print devices due to how the mechanism operates.

As a rule, single-sheet, front-loading inkjet printers roll the paper around the platen roller and print on the top side of the sheet. Mark a test sheet with an arrow pointing up, located at the top of the sheet, and then test the print using low quality to ensure that the orientation is correct.

Duplex manual-feed paper can be tricky as it is easy to feed in the paper upside down and the wrong way around:



HP inkjet all-in-one print device, front-loaded



# Quality

It used to be the case, with early daisy wheel and dot-matrix printers, that if you wanted to increase the quality, the print device performed a second pass over the line. The data comprising the output for the line was printed and then the print head ran back over the same line in reverse. Things are slightly more sophisticated now!

The quality of printout depends on the amount of ink used (which can be set in the printer profile), but also the output resolution. Standard PC monitor images use 72 dots per inch, whereas printed media requires much finer detail. Standard document printing is 300 dpi, with most high-resolution photographs and signage printed from 1200-2000 dpi.



# Device sharing

Print devices cannot be paired with a number of systems interchangeably using a variety of wired and wireless technologies. These are discussed in this section.





# Wired

A wired device is connected directly to a PC. It can be shared on the network by either physically disconnecting it and reconnecting it to another neighboring PC, which also has the device drivers loaded. However, this is cumbersome. Assuming that PC1 is to be left switched on, if the printer object within PC1's OS is shared then the print process can be managed by PC1 for others on the network. The printer drivers will be sent to the client PCs if needed, otherwise it is possible to configure PC1 as a print server--it will manage the print job on behalf of the other PCs.

In this example, the wired computer is connecting by LPT/Centronics cable.



# USB

If we re-plug the print device into a different USB port to the one it was originally installed upon, the OS will think that it is a brand-new printer and install a new printer object alongside that of the original one. The USB port is tied to the configuration used during the printer install, so it is important not to swap USB ports.

USB printing is much faster than using the line printer cable. Again, the print object can be shared across the network.

Be careful when swapping architectures--64-bit machines can run 64-bit and 32-bit printer drivers, and may need to send the 32-bit driver out to other PCs if not designated as the print server. A 32-bit machine can only run 32-bit drivers.



# Serial

A direct connection between two PCs can be achieved with a serial cable. This can be used to copy files from one PC to another. Unfortunately, the baud rate used is often slow and error-prone. Typically, you would use a COM2 (DB25) cable for this.

The advancement to this is to use a USB serial cable, which will auto-negotiate the connection and contains better communications protocols, ensuring the transfer is less problematic.



# Ethernet

By setting up a SOHO network using Ethernet cabling and the TCP/IP protocol stack, we can make use of the three-way handshake, speed contention, and error checking mechanisms built into TCP/IP to ensure that the transfer runs smoothly.

Where we are connecting two PCs directly to each other a crossover cable is used. However, if you have an auto-sensing switch, two patch cables (straight through) can be used instead, with the switch acting as an intermediary between the two PCs. The PCs must have the same subnet and be on the same numerical network (for example, 192.168.1.1 and 192.168.1.2 with a subnet mask of 255.255.255.0). Also, file and printer sharing should be turned on and the folder containing the file needs to be shared. PC2 will need to know a login account on PC1, which has been given sufficient permission for them to access the share, or be using a publicly accessible folder across the work group, such as a Homegroup folder.





# Wireless

In terms of configuration, wireless can be set up in infrastructure mode (where the same applies as the previous wired connection), or you can set up an ad hoc network such as a **Personal Area Network (PAN)**. Here you are using wireless connectivity to send directly to one other device. PANs are synonymous with smartphones, but are not used on office networks as security needs to be in place.



# Bluetooth

One such simple and fairly secure technology is Bluetooth, as most smartphones are Bluetooth enabled. A common PIN code needs to be known by both parties for the device to be paired to the neighbor device, but once done files can then be shared. Bluetooth is a fast, efficient solution for two people who trust each other to share a file.



# 802.11 - a/b/g/n/ac

The 802.11 standards in terms of speed and distance were referenced earlier in the chapter. Here we need to consider how to make them secure:

- **Stop broadcasting the SSID:** The station identifier is needed to connect your device to the network but once it is known and registered, why tell the rest of the world that there is a network present at all? The device can seamlessly connect to the network without the need for the SSID to be broadcast.
- **Use Wired Equivalent Privacy (WEP):** This is an encryption protocol introduced in 802.11b, which encrypts the packet using an **augmenting seed**. However, on its own WEP is easy to crack, so should not be the only solution.
- **Use Wi-Fi protected access:** This is an authentication system where a password known by both parties is used to connect and establish a connection session.

For larger networks where security is an issue, implement 802.1x certificate management. A certificate file can be used to either encrypt or authenticate the user. The same certificate has to be present on the sending and receiving computers.



# Infrastructure versus ad hoc

By setting up the wireless link in Infrastructure mode we can use some of the features listed preceding which are not relevant to a PAN ad hoc network.





# **Integrated print server - hardware**

By connecting the print device to a print server (either directly or across the network using an IP address) the server can manage all print jobs for that print device on behalf of other users. This means that other users do not need to install the printer driver on their own machines--the print request is rendered and managed by the print server.



# Cloud printing/remote printing

We can take the analogy further, by connecting into the corporate network from outside of the network, assuming that you have a domain trust or a cloud-connected domain, your network login account can feature several claims, such as the printer you can access and the level of access you can have. By connecting with a **DirectAccess** session, the session itself runs inside of the network, However, you manage your session from somewhere else, such as your home. Otherwise it is as if you are sat at your desk.



# Public/shared devices

There are wider implications for printing across PAN or public networks. These security questions are raised here.



# Sharing local/networked device via OS settings

The OS will have a network page where you can see all shared objects across the network--other PCs and their shared objects as well. In here, you can also enable file and printer sharing, if it is not already enabled, allowing you to discover other devices and their shares.

A shared folder has two security permissions assigned to it--one for the share and one for the folder itself as it resides on the disk (NTFS). The security permissions are cumulative--the most secure applies.





# TCP/Bonjour/AirPrint

**Transmission Control Protocol (TCP)** is an OSI layer-four solution that relies on a DNS server to discover the IP addresses of devices on the network.

The Bonjour service is a discovery protocol allowing the PC to find devices not currently listed. It uses a multicast Domain Name System to find the IP address and name of the devices that are in its neighborhood. Bonjour is common to Apple iOS systems and is installed when iTunes is installed, to offer support for smartphones.

**AirPrint** is designed to allow the user to print photos from their iPad, iPhone, or iPod without having to install any drivers. It is a suite of printer drivers, printer discovery systems, and a photo finishing app allowing the process of printing to and device without direct contact with the device.



# Data privacy

How secure data is depends on how secure you have made it. Should it be in a shared folder? Have I restricted access to only key staff, or groups of people? What access rights should other people have? Have I encrypted the file? Who else has my certificate/decryption key?



# User authentication on the device

A user can be authenticated by their retina pattern or fingerprint (**Extensible Authentication Protocol (EAP)** technologies), by a username and password stored on the local SAM database or in AD, or by a pin code or pattern swipe.



# Hard drive caching

The files stored on the hard drive are cached. This means that they are temporarily written to another area of the hard drive. The problem here is that I can use a low-level undelete program to access the temporary version of the file if the actual saved file is protected. In order to do this, however, I need to access your PC with sufficient privileges, or steal the hard drive.

To combat this, we turn off caching and also save our files onto a central file server.





# Video training

To summarize this section I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Configuring SOHO Multifunction Devices (9:37):** <http://www.professormesser.com/free-a-plus-training/220-901/configuring-soho-multifunction-devices/>



## **901.1.2 Comparing and contrasting differences between the various print technologies and the associated imaging process**

Sticking with print devices, we compare the differences between each type of printer. We consider how they work and the differences in their output, and look at specific hardware within the print device. Finally, we will consider how we can print by saving a file using a format that is easy to convert and send to a printer--virtual printing.



# Laser

A laser printer is so called as a laser beam is shone onto a rotating mirror capable of directing the beam at specific areas of a photosensitive drum. The sensitive areas attract toner (an ionized carbon/wax composite) to then be attracted to the paper as it passes by the drum. The toner is then sealed onto the paper via pressure and heat.

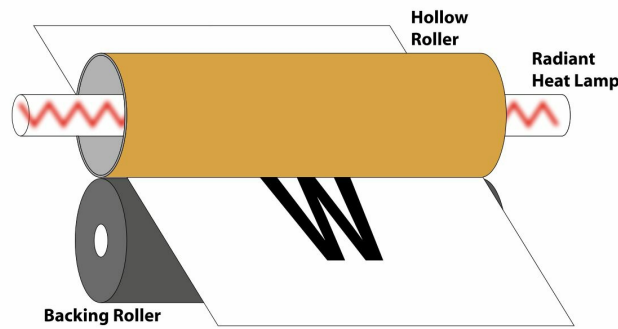
One sheet of A4 can be processed in a matter of seconds, making it an economical and cost-efficient solution at several thousand sheets per toner cartridge.

- **Imaging drum:** The photosensitive drum, once triggered by the laser light, causes toner to stick to those parts of the drum as the drum passes through the toner reservoir:



Imaging drum

- **Fuser assembly:** At temperatures of 200 °C, the fuser unit provides heat and pressure, sealing the unbonded toner onto the paper sheet:



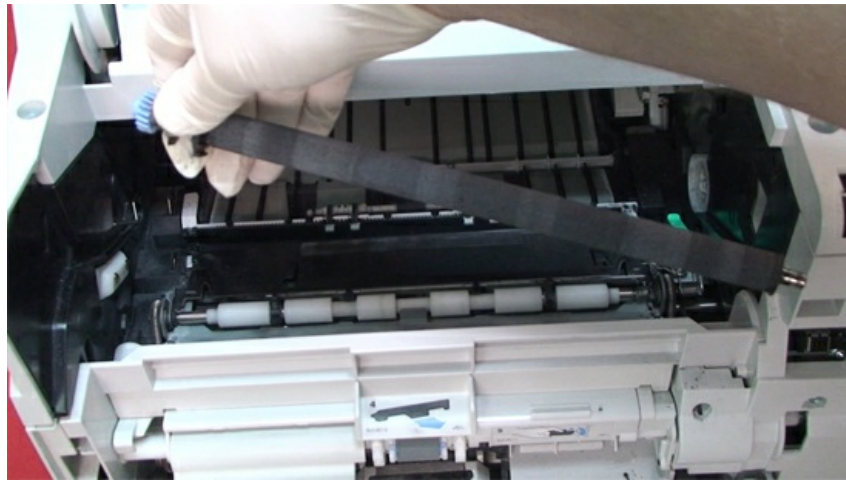
Laster printer fusing

- **Transfer belt:** Color laser printers use a transfer belt, which not only moves the sheet through the assembly, but also ensures that the paper does not move out of alignment during transit. The paper passes over the toner cartridges in turn and does not move out of alignment given that the rubber belt is able to hold the sheet in position (with friction or static electricity) so that the toner can be applied uniformly:



An electrostatic transfer belt

- **Transfer roller:** The transfer roller has an opposing electrical charge to the drum, transferring the toner onto the paper sheet. Any unused toner is also collected by this roller, where it is returned to the toner reservoir:



The transfer roller

- **Pickup rollers:** The pickup or feed roller is a large rubber roller (also known as the foot or finger as on some models the pickup is egg-shaped) capable of making contact, with high degrees of friction to the paper. In this way, the top sheet of the ream is pulled forward and into further pinch rollers (registration rollers), which carry the sheet uniformly into the assembly:



Pickup roller

- **Separator pads:** The stationary pad (separation pad) can be found preceding the pickup roller and is used to separate the sheets so that only the top sheet is carried into the assembly. The pad is often made of board or cork, and provides a counter-surface for the pickup roller, improving its performance. However, over time the pad wears down, causing doubles (a group of, or two sheets at a time) to be carried into the assembly, often causing a paper jam. The pad and pickup roller are common items to replace and replacement parts are common in a maintenance kit:



A separation pad

- **Duplexing assembly:** The duplexing assembly is capable of flipping the sheet so that the reverse side can be printed on the reverse of the sheet:



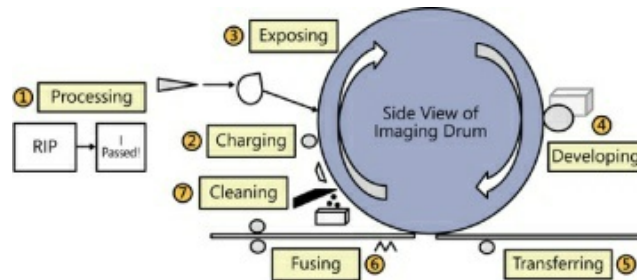
A duplexing assembly

- **Imaging process:** The laser imaging process is broken into the following steps, in sequence:
  1. **Processing:** Data is sent from the computer to the print device in a stream and format it can understand. This data has been spooled (sent at a speed accepted by the print device).
  2. **Charging:** The corona wire charges the drum with, typically, 600 volts DC. This enables toner to be attracted, and to stick, to the drum in the next stage.
  3. **Exposing:** A laser beam is shone at key areas of the drum where the image will be produced. This allows these parts of the drum to be sensitive and with the electrostatic charge applied only to the affected parts.
  4. **Developing:** As the drum turns, the toner is applied to the painted area of the drum.
  5. **Transferring:** The corona wire passes a positive charge from behind the sheet as the sheet passes by the toner-coated drum. The negatively charged



toner is attracted to the corona wire, but as the paper is in the way it falls into position onto the sheet.

6. **Fusing:** The sheet then passes through a heat roller assembly, which bonds (fuses) the toner onto the page.
7. **Cleaning:** Finally, the last pass of the drum is over a cleaning blade, which wipes off any excess, unused toner, which falls back into the toner reservoir:



The laser printing process



# Inkjet

Whilst a major part of this section is rightly devoted to the laser printing process, a number of other print systems are also in use. Inkjet remains a high-quality, low-production solution ideal for photographs and images. Here, we will look at the physical mechanisms within an inkjet printer.

- **Ink cartridge:** Here the ink reservoir and print head are the same unit and are housed onto an actuator arm, moving the head left to right, across the page:



CMYK colour dots

- **Print head:** The print head sprays a tiny mist of ink onto the paper. Different amounts of primary color inks (cyan, magenta, yellow, and black) form the specific colors as each jet points at the same point on the page. The print head also contains a chip with information as to how full the reservoir is, from original purchase.
- **Roller:** The platen roller sits behind the paper. The paper is rolled into a C-shape and held in tension as the ink is applied. The area between the print head and paper is held in tension.
- **Feeder:** Typically, a plastic back plate at the top of the printer allows gravity to keep the paper in position. The feeder roller and separation pad are at the base of this plate, passing a single sheet at a time into the assembly.
- **Duplexing assembly:** As with the laser printer, a sheet of paper can be turned over and the opposing side fed into the printer, where the reverse side data is printed.
- **Carriage:** The carriage return is a motorized belt suspended around two metal runners. The carriage is a plastic assembly that holds the print head in place. The carriage assembly therefore moves the print head from left to right in front of the paper.
- **Belt:** As part of the carriage return is a rubber belt, driven by the motor, which turns the belt clockwise or anticlockwise to move the carriage left to right along the track.
- **Calibration:** If stopped by the user, or if a foreign object gets in the way, it is possible for the belt to slip a groove, especially if the open carriage button is pressed (used to replace the cartridge. This moves the carriage into the center of

the track to allow for easy access.). Calibration is therefore two things:

- The ability to reset the carriage assembly so that the start of the motor's cycle is when the carriage is at rest in the housing, against the cleaning pad, and that a full run takes the carriage to the end of the paper, and
- The ability to use a printed sheet to re-align the appropriate print nozzles so that the CMYK dots correctly overlap (as described previously).



# Thermal

The key components of a thermal assembly are:

- **Feed assembly:** A pinch roller pulls the paper from the reel into the assembly. One side of the paper is chemically coated to respond to heat from the element.
- **Heating element:** The heating element is able to heat specific parts of the paper, which chemically react and sublime (change color).
- **Special thermal paper:** The thermal paper reacts only in the areas exposed to the heat from the element. At these points the dye is visible on the page.



# Impact

The old stalwart of impact printers has always been part of the CompTIA course and rightly so. These printers just work and have been used without significant change to the printer technology since the 1970s. Here we may homage to early systems such as the daisy wheel printer, but more significantly focus on the dot-matrix printer.

- **Print head:** Impact is a common term to describe daisy wheel and dot-matrix printers where a solenoid fires a series of pins in a pattern to look such as a letter, or number. With daisy wheel, it is the same process, but a **slug** (that is, a metal hammer with the font embossed on the hammer head) is swung forward, making impact with the paper and leaving an impression. The print is formed character by character working across the line.
- **Ribbon:** The ink ribbon sits in front of the paper. The impression presses the inked ribbon onto the paper leaving an impression. The key factor here is the platen gap - the distance between the print head and the platen roller behind the paper - too close and the paper may be torn, but if the print head is too way away, a faint impression may be left, or no impression at all.
- **Tractor feed:** As preceding, the paper is stored concertina-fashion in a box. The edges have perforated sections known as the track. The platen feed roller has a series of fingers that evenly pull the paper into the assembly.
- **Impact paper:** Paper can be sheet-fed through the registration rollers and into position within the assembly. The printable area is defined by the extremes the print head can move to. It is important, therefore, that the paper is calibrated from character position 1, so that a margin is left. The paper feed section has two metal fingers either side of the sheet designed to keep the sheet central relative to the platen roller and assembly, and to ensure that the paper is fed in exactly straight.





# Virtual

Not all output is printed. Virtual printers are in fact driver files tricking the OS into showing a conversion engine as though it was a real printer. The resulting output is a formatted file which can then be used by the end-user, or attached to an email. Since the fact that Office 2010 now supports XML and PDF printouts for editing the need for virtual printers has reduced, but they are still used.



# Print to file

Not all print devices print to actual paper.

A Virtual printer is a print object within the OS capable of converting a file into another format, where it can then be used by another program. In this way, files can be converted from a proprietary format to a more generic format.



Did you know that Microsoft Office 2013 and higher print natively to PDF so there is no need for a third-party virtual driver?



# Print to PDF

The most common document format is the PDF invented by Adobe. This contains metadata about the file and security information restricting access to the file to certain users.

Modern PDF files are also editable as a form where specific fields have been highlighted. The user can then complete a form with key information--crosses in boxes and text in type fields. At the end of the form is the facility to add a signature either in the form of a picture, a signature (using a mouse, or more accurately, using a pen and digital pad), or by adding a digital signature--here, the software uses the given full name and adds a visual, italicized generic script version of the signature, but more importantly, creates and adds to the file a digital signature containing the date and time stamp, and key information about the user, which can be used as evidence against a non-repudiation attempt.



# Print to XPS

Microsoft's equivalent to PDF is the **XML Paper Specification (XPS)**. XPS is not based on the PostScript language (common for sending true-type fonts and printer management information).

Should I use PDF or XPS? XPS was introduced in Vista, but never really got off the starting block as PDF was already synonymous and XPS didn't really solve any problems. Instead, Microsoft offered support for PDF editing on Microsoft Office 2010/2013/2016, and now we save PDFs and don't really worry about the format.

XPS viewer can be added to a server as a feature.

We have a problem here. PDFs opened in Word 2010 strip off the custom data added to the form and repaginate the form! Not a good idea. If you need to fill out a form saved as PDF use Acrobat Reader. Early versions required Adobe Acrobat (the editor), but now forms can be set to be edited in Acrobat Reader.

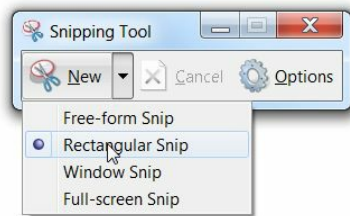




# Print to image

If necessary, a PDF can be converted to an image file (a bitmap). The fonts are rasterized into pixels and therefore no longer recognized as text. This, however, is useful if you need to take a capture of part of a document.

The easiest way of doing this is to use Microsoft's **Snipping Tool**, which allows you to take an area of the screen and save this as a new image:



The Windows Snipping Tool



# Video training

To summarize this section I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Understanding Laser Printers (9:00):** <http://www.professormesser.com/free-a-plus-training/220-901/understanding-laser-printers-2/>
- **Understanding Inkjet Printers (5:03):** <http://www.professormesser.com/free-a-plus-training/220-901/understanding-inkjet-printers-2/>
- **Understanding Thermal Printers (2:22):** <http://www.professormesser.com/free-a-plus-training/220-901/understanding-thermal-printers-2/>
- **Understanding Impact Printers (3:36):** <http://www.professormesser.com/free-a-plus-training/220-901/understanding-impact-printers-2/>
- **Understanding Virtual Printers (4:24):** <http://www.professormesser.com/free-a-plus-training/220-901/understanding-virtual-printers/>



## **901.1.3 Given a scenario, perform appropriate printer maintenance**

As a first-line support or IT technician, two things take up most of your time--resetting passwords and maintaining print devices. In this section, we will consider some of the problems you will encounter and how we can resolve them for different types of print device.

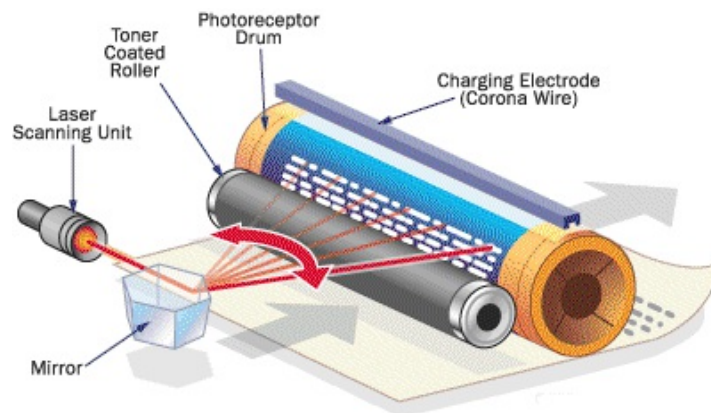


# Laser

Laser printers will be covered in greater detail in a later module. For now, it is worth knowing that the laser printer can print a high-quality image; a font of any size and type now that we use true-type fonts. The font data is in fact rendered within the PC, whereas early printers required the use of a font cartridge within the printer itself. We now not only render but spool the data stream at a speed the printer can cope with.

Laser printers use a laser beam on a turning roller. This photosensitive roller has the circumference of one third of an A4 sheet. As the sheet is fed into the printer, the drum is cleaned of excess toner from the previous turn, the roller is charged, and toner is attracted to the drum and sticks on the sections exposed to the laser light. Excess toner falls back into the reservoir. The paper passes between the drum and the corona wire. Toner is attracted to and sticks to the paper.

The paper then passes between a heated roller, which warms the toner (a combination of a low temperature-melting wax and ionized carbon), which then sticks and dries to the page:



Laser printer principles

- **Replacing toner:** When the toner cartridge is running low, the toner may be unevenly distributed. You can often get a few more sheets out of the printer by gently shaking the cartridge so that the toner is evenly distributed across it, then re-adding the cartridge.

A typical toner cartridge will last for 1,000 to 10,000 prints (sheets), making the laser printer the most economical device on the market.



To replace the toner cartridge, the cartridge is removed from its packaging and then placed into position within the reservoir. The plastic seal tape across the front of the cartridge can then be pulled back, releasing toner forward.



Please be careful with toner! It is carcinogenic and very easy to get on your fingers and clothes.

- **Applying maintenance kit:** A maintenance kit is a selection of replacement parts:
  - Fan exhaust gauze/HEPA filters
  - Q-tips for cleaning internal areas of the mechanism
  - A replacement cork board for the feeder roller
  - A replacement feeder roller
  - A replacement heating roller

High-production laser printer models and photocopiers have a sheet counter (such as a milometer on a car), which counts the number of sheets printed. After the maintenance kit has been correctly applied, the engineer's final job is to reset this counter as essentially, this is a reconditioned machine.

- **Calibration:** As with other print devices, the laser printer has to be calibrated. A manufacturer-provided sheet can be scanned and used to reset components to their default settings. However, the process of re-powering the laser printer will reset mechanical components to their initial positions.
- **Cleaning:** The external and tray areas should be cleaned with a dry cloth and compressed air to remove dirt, dust/debris, or paper residue. However, be careful not to apply compressed air near to the toner reservoir as the toner may then be breathed in.



# Thermal

Thermal paper uses a heating element/wire to make contact with chemically treated, heat-sensitive paper. The most obvious example of this is modern shop sales receipts:

- **Replace paper:** The paper is wound as a roll and added to the printer, which pinches the paper through the platen. Near to the end of the roll a red stripe can be noticed, which indicates to the user that they are approaching the end of the roll, which should soon be changed.
- **Clean heating element:** The heating element should be kept clean and debris-free to ensure a consistent printout. A printer kit can be used to clean the element.

Naturally, disconnect the power and leave the printer for some time for the element to cool down before you attempt to clean it. Never use liquids, but simply a dry cloth. Avoid knocking the element out of its position.

- **Remove debris:** The print roll is enclosed within the device. Friction causes flecks of paper to break off and stick inside the machine, along with dust from the exterior. Over time, the heating element will attract some of these particles, which will seal onto the heating element/wire and need to be cleaned with a print-cleaning kit. If this does not happen, areas of the printout will be darker (or lighter if heat is obstructed from reaching the paper):



A sample till receipt (thermal paper)

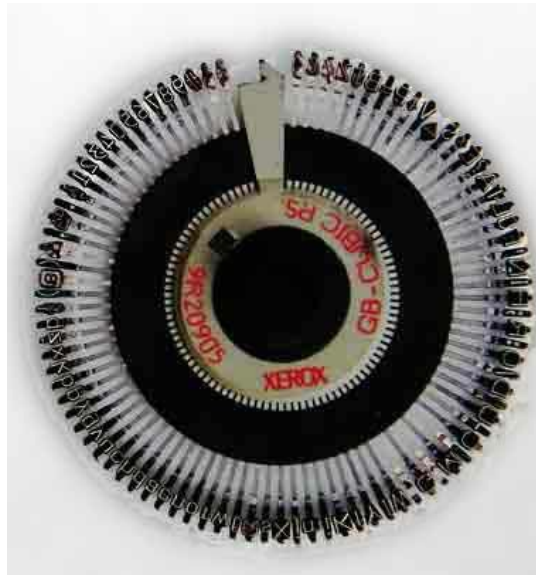


# Impact

The impact printer describes a family of now very old print devices where a hammer, or print head, fires against an inked ribbon. The impact presses the ribbon against the paper and the additional impact is absorbed by the platen roller

Typical impact printers include:

- **Dot matrix:** A matrix of pins forms the print head. A solenoid pushes the pins out of the print head at a high velocity, where they impact on the ribbon leaving a mark on the paper in the shape of a dot. The sequence of dots resembles a letter or number. The print head works one line at a time, one character at a time. One line may take up to three seconds to print.
- **Daisy wheel:** Now defunct, the **hammers** or slugs impact forward and make the impression of the character selected. As with dot-matrix, the printers work one line at a time, one character at a time:



Daisy wheel printhead



If you wanted to change the font size or type, you needed to take a spanner, unscrew the daisy wheel, and replace it!

- **Replace ribbon:** The ink ribbon often lasts a very long time, but over time will dry out. Ink will also be transferred onto the paper, so the ink ribbon moves on one character at a time.

The ribbon is fed through a feed and take-up spool, and is fed under a guide and held in place in front of the target zone:



Inkjet ribbon (from a typewriter)

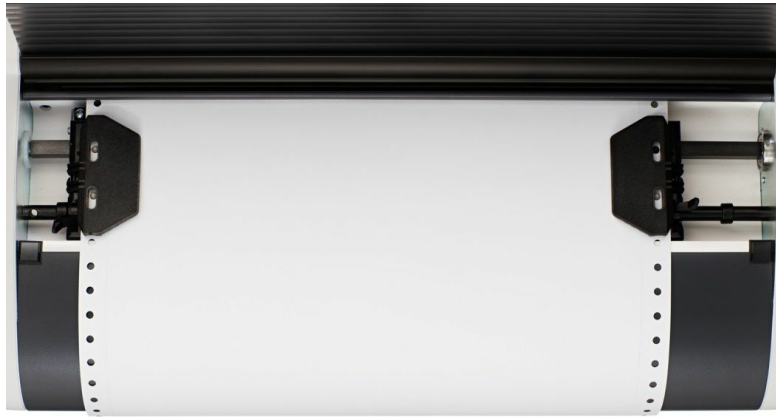
- **Replace print head:** For dot-matrix or daisy wheel, the head can be unscrewed and replaced like-for-like. First power off the device and remove any covers that may be obstructing the head. Move the head manually into the middle of the track and then remove the data-control cable from the head. Unscrew the head from its mounting and replace like-for-like.
- **Replace paper:** There are two types of paper you can associate with typical SOHO printers--tractor feed (for dot-matrix) or sheet-fed.

Sheet-fed paper simply needs the user to add more paper to the paper tray. For top-loading inkjet printers, gravity feed keeps the clutch of paper in contact with the feed roller, which makes contact with the top sheet, pulling it only into the mechanism where it is pinched to the platen.

Always fan the paper, ensuring that you get airflow between each sheet. To do this, take only 10 to 20 sheets and hold both ends tightly between your finger and thumb, at both ends. Bend the paper 180 degrees and reposition the one end so that the hold on the paper is uneven. You will see that the paper has now separated. Further fan the paper at one end to ensure that air goes in between each sheet. Now, knock the paper back into one block and add it to the tray/feeder.

Tractor-feed paper contains perforations at the top and bottom side. The paper is Z-folded into a block. The edges contain a 1cm margin containing punched holes. The printer contains a feeder roller with pins on either side, which will make contact with the holes and pull the paper down into the printer, toward and

around the platen:



Tractor feed printer





# Inkjet

The inkjet uses a similar delivery system to the early dot-matrix. Sheets are fed in singly, wrap around a platen roller, and the print head sprays a fine mist of ink. There are typically four primary colors used (cyan, magenta, yellow, and black). The ink dries quickly and the printer head moves left to right along a motorized track, printing one line at a time.

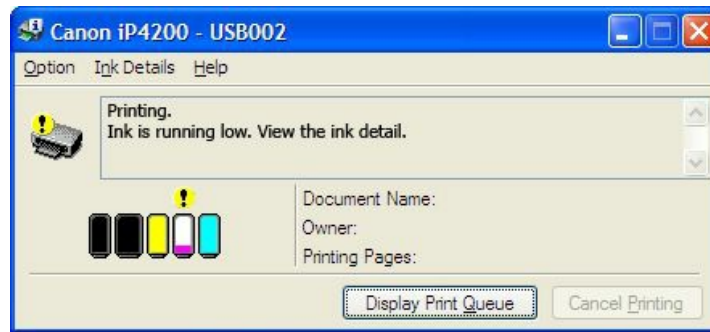
- **Clean heads:** Periodically, and after disuse, the ink will dry on the print head, clogging the nozzles. The printer has a print cycle which can remove dry ink by wiping the head against a sponge and spraying fresh ink to check that the nozzles are clear. This process does, however, waste ink, so should be used sparingly:



HP inkjet cartridge and printhead with nozzles

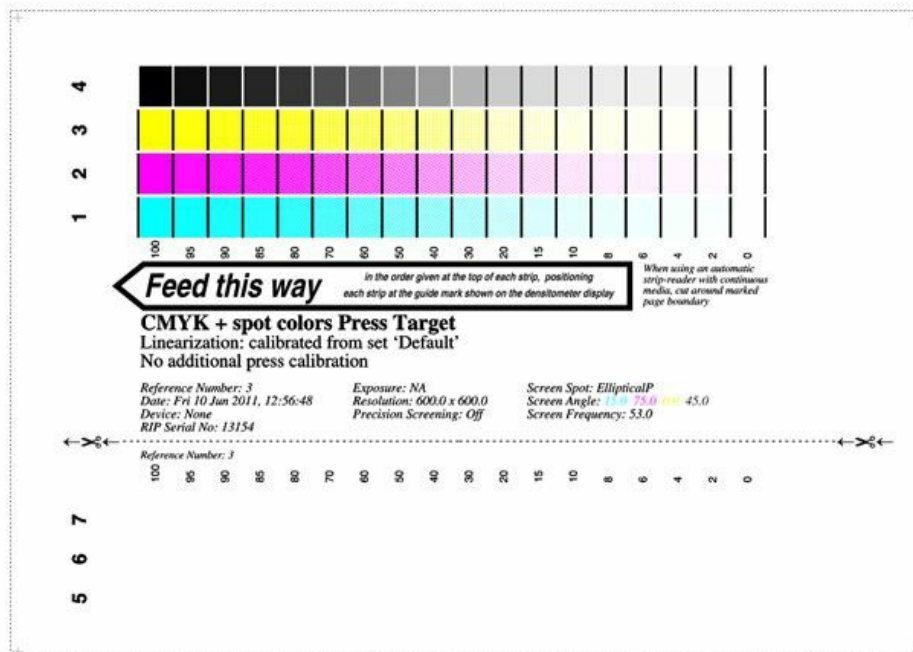
- **Replace cartridges:** Typical HP cartridges are actually only filled one third full, although you can purchase completely filled cartridges. The cartridge contains a chip, which contains information on how full the cartridge is and how many sheets can be printed. This information is fed back to the printer software on the OS, notifying the OS when the cartridge requires attention or is empty.

Modern cartridges, although they can be refilled with fresh ink, will need this chip to be reprogrammed in order to update the printer software, otherwise the OS will still think that the cartridge is empty:



Ink cartridge empty alert

- Calibration:** Once a new cartridge and print head is installed, the nozzles will not be aligned to print in the correct place on the page. The process of moving the cartridges subtly to ensure that all four are aligned is referred to as calibration. A calibration sheet is printed and then re-scanned in. The calibration sheet is read in to determine how far out from central alignment each head is; the printer will then automatically correct the position of each head:



Inkjet calibration sheet

- Clear jams:** A paper jam is typically caused when more than one sheet is pulled through into the printer by the feed roller, or when you are printing multiple pages and the completed page is obscured and cannot cleanly leave the print mechanism. In this case the next sheet being fed in is obscured, or knocked out of alignment as it is friction-grabbed (pinched) by the feed roller and fed around the platen roller.

A jam is typically cleared by canceling the print job and pressing the eject paper button, which ejects one sheet's worth of paper. If this is not successful, it is a manual process of gently teasing parts of the jammed paper out of the assembly and moving the print head out of the way.

When the print head has been disturbed, it is common to have to reset the print head to its starting position by powering off, then powering on the print device:



A paper jam

Jams are also caused through exposure to high humidity levels. Here, the paper has soaked up moisture in the air, making it more fibrous and susceptible to tearing, as well as increasing its thickness as the fibers expand. If a pickup roller is set to pick up one sheet of 110 gsm it may instead pick up two, or for the paper to be fed through into the assembly out of alignment, or if damp, for a part of the paper to break off and get stuck inside the printer.



# Video training

To summarize this section I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Maintaining Laser Printers (4:44):** <http://www.professormesser.com/free-a-plus-training/220-901/maintaining-laser-printers/>
- **Maintaining Thermal Printers (2:42):** <http://www.professormesser.com/free-a-plus-training/220-901/maintaining-thermal-printers/>
- **Maintaining Impact Printers (2:22):** <http://www.professormesser.com/free-a-plus-training/220-901/maintaining-impact-printers/>
- **Maintaining Inkjet Printers (3:15):** <http://www.professormesser.com/free-a-plus-training/220-901/maintaining-inkjet-printers/>



# Summary

Overall, in this chapter we have looked at all of the hardware aspects of the system, of external peripherals, and print devices. To get you ready for the exam, this chapter covers a great deal of technical information but is also pragmatic--it explains how components differ, where they can be found, and how they are used from an end-user and business perspective. We have delved in some detail into the electronic aspect of the system, listing key terms that are common within the industry.

Remember that all of this started from the IBM PC and from this blueprint, variants were created as manufacturers vied to compete with ever-better communication standards. These new technologies have had to be reigned-in for a number of reasons, and standardization has been critical. The humble USB port is now synonymous with all devices for this very reason.

Okay, so you know about one PC. In the next chapter, we will consider how we can connect two or more together to make a network. This next chapter is exciting as we can now share data, and we will explore how this is done electronically as well as from an IT perspective.





# Networking (901.2)

This chapter focuses on how a PC or other end user device can communicate with other devices on the network. There are a few assumptions here, such as you are already familiar with the concept of the **Open Systems Interconnection (OSI)** model. This is used in network design and troubleshooting to establish at what level within the network a problem may be occurring.

All network devices conform to some degree to OSI. While cables may simply send an electrical, audio, or light signal (layer 1), the actual binary data sent in bursts (blocks, cells, or frames) is managed as devices talk to each other to establish if they are ready to receive a connection and then to gracefully close the connection when complete (layer 2). We add our own numbering system to define portions of the network (layer 3) and what type of data we are sending (layer 4). Our operating system splits the connection into separate pathways and tries to get the best speed out of the network, sending pieces of the file through different routes, managing each route (layer 5). The data is often encoded and may contain text that is language and encoding-specific (layer 6, for example, Pretty Good Privacy).

Finally, our data is used by an application that the end user can work with (layer 7).



The Open Systems Interconnect (OSI) model

We will look at the various network connectors and cables used, comparing them in terms of practicality, speed, and distance. We will look at the TCP/IP protocol stack used to manage the data across the network. We will cover different wireless protocols

and compare them in terms of speed and distance. We then consider the domestic/SOHO network and contrast its hardware to that used across an Enterprise network. Looking beyond the building, we consider the cables and connections used within the wider infrastructure and consider different network designs. We then focus on the dedicated hardware used within an Enterprise network. Finally, we consider the various network-specific tools an IT technician may use and consider different scenarios where these tools are used.

We start by looking at a variety of network cables and connectors used, then will compare how cables are wired and techniques used to minimize interference. We then look in some detail at the TCP/IP protocol stack, especially how this is used alongside DHCP and DNS. WE focus on network ports, then cover Wi-Fi standards. From a SOHO perspective, we consider the basic network elements and then we consider media connection types such as satellite and cellular networks. We then look into logical network types, then move into a detailed look at network hardware. Finally, we look at the variety of network testing tools used to check for and alleviate problems on the network.



## **901.2.1 Identify the various types of network cables and connectors**

In the previous chapter, we considered what makes a PC and how we can extend a PC, or share data from it to its connected devices (for example, a printer). Here, we will look at not only how we can share data but also resources and software services across a network of 2 or more PCs.

The model to have in mind is the concept of a domain (client-server) network. Most SOHO networks are in fact a workgroup (peer-to-peer. Each PC is independent of each other.) In the domain model, one central server offers a service to all of the other client PCs. End users can share the same service (for example, a file server) and many people access the same service at the same time.

We will start by looking at the physical network wiring used to connect PCs together, including the connectors used. You will be introduced to the TIA wiring standard, used when making up your own Ethernet cables.



# Fiber

Fiber-optic cables consist of a strand of glass or plastic material that will carry a light beam. The process of sending light across time produces a signal that can be re-coded as a binary data stream. By sending light of slightly different frequencies, it is possible to send several light signals across the same medium at the same time. This process is known as multiplexing. Each light signal is decoded and re-coded as a digital binary electronic stream. Fiber-optic cables actually consist of two sheathed strands, even though we refer to single mode. This is because one cable strand sends the light stream one way while the other sends returning data in the opposite direction.

The fiber cable attaches to two ports, one of which is laser or LED emitter and the other is a light sensor capable of receiving and decoding the various signals.





# Connectors: SC, ST and LC

Fibre connectors are used with specific types of cable and are remembered by how they are operated, as common names have now developed for these connectors:

- **ST (straight tip) common name--shove-twist:** The ST connector encloses the cable in a rubber sheath terminating with a bayonet cap to lock the cable in place. It is commonly used with multimode cables, but can be used with either type.
- **SC (standard/subscriber connector) common name--shove-click or square connector:** The SC connector ends with a gray plastic coupling, and a dual plug attaches the cable pair into the receiver/transmitter unit (a dual SC), although it is common to also buy SC plugs that are for each individual cable. SCs can be used with either cable mode type.
- **LC (lucent connector):** This connector is ideally suited for single mode cables, although both versions are again compatible. It sends in a dual gray plug with ceramic ferrules at the tip of the fiber on each cable. An LC is half the size of an SC connector. It is again square shaped and has a locking clip on the top of the plug. The ferrule is half of the diameter of an SC connector. Given the size difference, it is possible to increase the density of fiber connections within your switch room. An LC is used typically with single mode cables only.

Which types of connector work with multimode cables, and which work with single mode cables? This is a difficult question to answer as this is defined by the interface, and the connector is basically a plug. A good reference for this is the Fibre Optic Cable Shop ([www.fiberopticcables.com/fa.html](http://www.fiberopticcables.com/fa.html)) who, on their site, list the ports available:

- **Single mode:** ST, SC, LC, FC (FC is similar in design to a BNC connector)
- **Multimode:** ST, SC, LC



# Twisted pair

Whereas fiber-optic cables are typically used within the backbone of the office building to connect floors together, or to connect sites together each floor contains an **intermediate distribution frame (IDF)**, or cabinet, that contains a patch panel and a switch, connecting each Ethernet socket (wall point) to a centralized area where all of the data will be collected and uplinked via one cable to the rest of the network.

Typically, the bandwidth here is smaller, with 100 Mb/s as the standard for a Category 5 (Cat 5) cable over 100 meters. For Category 6 (Cat 6) cable (mostly found as the standard within the US), 1 Gb/s, known as Gigabit Ethernet, is now commonplace.

Ethernet cabling consists of eight sheathed copper wires, terminating with RJ-45 connectors. Unlike fiber-optic cables, where light signals are sent, an electrical charge is sent across the data transmission wires. As with the light in fiber-optic cables, we are sending a binary signal.

In the IDF, or cabinet, the patch panel is typically a 110 block. It is used to connect the Cat 5 cables running to the connection points in each room on the floor through to the patch panel, where each socket can then be wired into the switch. The 110 block is a series of metal v-shaped blocks that capture and cut into the plastic surround of the wire, therefore making the connection while also holding the wire in place. Each Cat 5 cable connects to a series of blocks that, in turn, are connected to the patch panel. In order to attach the wire to the block, a **punchdown tool** is used to force the wire into the slit, making the process of attaching the cable relatively easy. **110 blocks** are preferred over the older 66 blocks as they produce less crosstalk.

The family of copper cables used within networking are often the more significant medium - they are found within almost all networks and can produce excellent local speeds. Copper is also the medium of choice for cost reasons as the cable is relatively inexpensive in comparison with other network media.



# Connectors: RJ-11, RJ-45

These are two main cables that we will consider as the twisted pair and the coaxial cable:

- **RJ-11:** The Registered Jack type 11 is a small, clear plastic plug with four gold/copper pins on one side and a locking clasp on the other. Of these, only two are typically used for standard analog phone networks, although all six are usually wired. For the UK, it is common to only see four wires in use. The RJ-11 is used to attach a serial connection to a device such as a managed router, but is more commonly used for connecting to a modem to allow connectivity between the PC and the telephone line. A second RJ-11 line is used to plug in the telephone as a monitor device and also to enable the telephone to operate normally when the modem is not in use.

In the UK, British Telecommunications (BT) have held the monopoly over the telephone network throughout the 1980s and 1990s. BT developed their own equivalent phone connector plug based on RJ-11, but which has a wider connection. Typical Asynchronous Digital Subscriber Line (ADSL) filters still have a BT jack and BT female input, but will use an RJ-11 input for the digital DSL signal.

- **RJ-45:** Registered Jack type 45 is the most common network port. This is the standard Ethernet connection port as found on NICs, hubs, switches, and routers. The RJ-45 is the common connectivity standard for connecting any network device. It consists of four pairs of twisted-pair wires arranged in the configuration 568A or 568B at both ends. This creates a straight-through or patch cable capable of adding the device to the existing network.

By mixing 568A at one end of the cable and 568B at the other end of the cable the swapping of wires 1 (end A) and 3 (end B) and 2 (end A) and 6 (end B) creates a crossover cable. This is used to connect together devices of a similar type where a data loop is required to create a circuit between the two nodes. This is typical if you were to connect two routers together, or two PCs directly to each other.

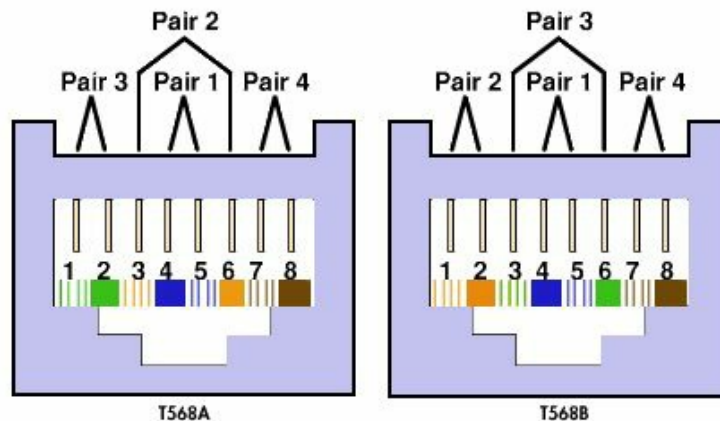


RJ-45 network and RJ-11 phone connector



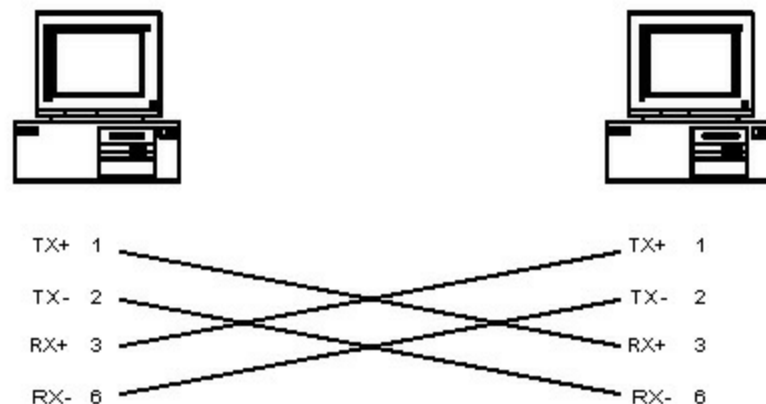
# Wiring standards - T568A and T568B

Also referenced in section [Chapter 6](#), Hardware and Network Troubleshooting (901.4), the TIA standards refer to wiring designs used across the industry. The T568A or T568B standards are interchangeable, but it is expected that as an electrician you are consistent. Typically, the T568A standard is used to wire the section from the wall socket through the plenum void space and into the patch panel (110 block). The T568B standard is used wherever a crossover cable is needed.



EIA/TIA 568A and 568B Standards

Remember that modern switches and routers contain switch-sensing hardware and can check if there is electrical connectivity; otherwise, switch pins within the device to compensate. The only need for a crossover cable in modern networking is to directly connect two PCs together, not using a switch in the middle.



Crossover cable diagram with 2 PCs directly connected



The U.S. government requires the use of the preferred T568A standard for wiring done under federal contracts.



**Reference:** <https://acuitysupport.zendesk.com/hc/en-us/articles/210113548-What-is-the-difference-between-T568A-T568B->

It is advisable not to mix the two color schemes, rather to use one (for example, T568A) and stick to it, using T568B only for the other end of cables to make crossover cables, rather than patch cables.



# Coaxial

Moving on to other network types is good-old ol faithful, the coaxial cable. Coaxial was first used in telecommunications for radio transmitters and audio devices. It is famous for the fact that the single copper wire is heavily protected from damage due to its protective plastic covering, then a copper braiding which earths the entire cable (at least connecting the earths of the two devices together, which should then separately be earthed to ground through the mains cable). The braiding shields the signal from a lot of EMF interference, **BUT NOT COMPLETELY**. This is why fibre optic is always the better answer in an exam question, but coaxial does have its place. The signal can stretch for long distances and supports in a fibre-to-premises network design.



# BNC

The **Bayonet Neill-Concelman (BNC)** or bayonetconnector (also commonly known in the UK as the **British Naval Connector** due to its use on UK naval vessels in the 1920s for use on radio communications equipment) is a standard connection type used with coaxial cable.

The main copper wire makes a connection with the metal tube to which the signal is sent. On the outside of the BNC is a quarter turn screw with a track cut into the outer collar to form a lock. This locks against two pins on the female end.

It is common to not only find a BNC connector in networking but also, due to its versatility, the 50-ohm BNC is commonly used in the broadcasting industry for TV, editing, and also for radio production.



# F-connector

The F-connector is a similar sturdy connection allowing the middle copper wire to be locked into position. Here, the F itself is a hexagonal threaded ring that locks the cable into place. It is commonly found on the rear of satellite and cable TV set-top boxes. Both are used with copper RG-58 and RG-59 cabling.



ohm copper coaxial cable with shielding. Notice the copper central wire





# Exam questions

1. I want to make a crossover cable. Which four pins are used?
  1. 1
  2. 2
  3. 3
  4. 4
  5. 5
  6. 6
  7. 7
  8. 8
2. Which is commonly used to create a backbone, connecting switches on each floor together?
  1. Coaxial
  2. RJ-11 phone cable
  3. Multimode fiber
  4. Single mode fiber
3. Which TIA standard is considered to be the default for networking within buildings in the US?
  1. T568A
  2. T568B
4. In which domestic devices is it common to find F-connectors?
  1. Satellite TV
  2. Cable TV
  3. Cable router
  4. ADSL router
  5. Dial-up modem
  6. Wi-Fi access point
5. How many wires typically form a FDDI ring?
  1. 1
  2. 2
  3. 3
  4. 4



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide.

- **Network Connectors (6:10):** <http://www.professormesser.com/free-a-plus-training/220-901/network-connectors/>



## 901.2.2 Compare and contrast the characteristics of connectors and cabling

Starting at OSI layer 1, the physical layer this section is going to focus on the transmission media through which we send our signal. While air (light, sound, or radio waves) is straightforward, each cable has an electrical and industrial standard and we are going to consider each of these in use on modern large enterprise networks.

Why is this? Why study enterprise-network design when I am working on end user products? Most end user products at some point will connect to the larger network, and as a first-line support technician you will need to learn not only the end user devices but how they connect to the rest of the network. Your career path will have in mind the fact that your next steps, after you certify with A+, will be to consider the bigger picture-- that is, the enterprise network.

We will start by looking at the two different fiber-optic cable modes and how they are used to send a light signal across a cable at high speed and over longer distances than is typically possible with Ethernet without the use of repeater boxes. We will then look at the different versions of Ethernet cable available to us and how the cable can be impacted by other signals, causing interference, and how shielding can help to minimize this. We will consider where the cable is laid within the building itself and how we can use a version of Ethernet cable designed to, in the event of a fire, produce gasses which are non-toxic.

Cabling data transmission speed can be affected by the distance the signal has to travel. Equally, when we consider the frequencies used for ADSL broadband, the quality of the signal would be impacted if telephone audio was sent on the same cable as the ADSL data without blocking the audio data from impacting on the higher-frequency data signal.

We will consider coaxial cable as well as twisted pair. We look at the speeds and distances possible with this cable and how it is still used by satellite and cable TV service providers, as well as with CCTV.



# Fibre

There are two main types of cable:

- **Single mode:** Here, a high-quality strand of glass or plastic is used to transmit signals over a long distance (up to 40 km). Single mode is high-speed and long-distance, but is usually only found within metropolitan networks, or within the telecoms infrastructure to carry trunk (bulk) data. The core glass fiber is cladded by a plastic sheath that traps the light inside, ensuring that the light emission is not lost in transit (total internal reflection).
- **Multimode:** This is more commonly found within one building, or between neighbouring buildings. Speeds are slower and the data distance is also shorter. The cable is made up of several strands of plastic or glass, each of which is capable of carrying a signal over a short distance. The light rays bounce off the walls of the core strands, allowing for several rays to be sent at the same time as a multiplexed signal; however, it is only effective at short distances.

Remember the difference. A single fiber usually carries a trunk signal comprising several different PCs' data combined onto one line. It is typically site to site and works up to 40 km. Multimode has several strands of fiber each making up the signal and is used within the building to connect floors together, or the IDF to the main distribution frame, where the data will then exit the building.





# Speed and transmission limitations

The speed of a cable is dependent on its ability to keep a pure signal and for this to be read correctly at the other end. Energy is expended as the signal travels down the cable, but if the power is not sufficient and the cable distance is too great, this power reduces due to resistance in the wire (in the case of electrical energy sent across copper cable) to a point where the signal at the other end is too weak to be read correctly.

To solve this problem repeaters, devices whose job it is to regenerate the signal, can be placed at key points along the transmission, boosting the signal and regenerating the clear signal, allowing for attenuation.

Speed [Mbit/s]	Distance [m]	Name	Standard / Year	Description
10	100 (nominally)	10BASE-T	802.3i 1990	Runs over four wires (two twisted pairs) on a Category 3 or Category 5 cable. Star topology with an active hub or switch sits in the middle and has a port for each node. This is also the configuration used for 100BASE-T and gigabit Ethernet. Manchester coded signaling.
100	100	100BASE-TX	802.3u 1995	4B5B MLT-3 coded signaling, Category 5 cable copper cabling with two twisted pairs.
1000	100	1000BASE-T	802.3ab 1999	PAM-5 coded signaling. At least Category 5 cable with four twisted pairs copper cabling. Category 5 cable has since been deprecated and new installations use Category 5e. Each pair is used in both directions simultaneously.
	100	10GBASE-T	802.3an 2006	THP PAM-16 coding. Uses category 6a cable.
	≥30	40GBASE-T	802.3bq	under development, uses encoding from 10GBASE-T on proposed Cat 8.1/8.2 shielded cable

Ethernet maximum distances

For Cat 5, the maximum distance is 100 meters. In practical terms, Cat 5e (e = extended) is slightly over this but the standard still lists this as 100 meters, although distances of 125 meters are possible. Note that this is an unbroken vertical or horizontal drop, without bends, from port to port.

Making a direct contact from end to end, unbroken, is not that easy. In the case of BNC or F-connectors the connection is tight, although it can loosen over time, causing loss of data if the wire becomes disconnected. With RJ-11 and RJ-45 there is a plastic retaining clip to keep all of the pins in place against the NIC. The problem, however, is with

fiber-optic cabling as there must not be any air gap between the ferrule (the plastic tip of the connector) because, otherwise, the light beam will bend and not hit the receiver correctly. Imagine an image entering the eye. For a normal-sighted person, the light hits the lens and is focused onto the back of the eye where it is sent as signals to the brain. For an astigmatic (short-sighted person), the shape of the eye is slightly bent, causing the focal point to not hit the correct spot. In fiber cabling, the air gap will cause the light beam to bend, or not hit the receiver at all.



You can refer to this video for a demonstration on how to fit an ST connector:

YouTube video demonstrating how to fit an ST connector (<https://www.youtube.com/watch?v=-0q6dBkBwJQ>)



# Twisted pair

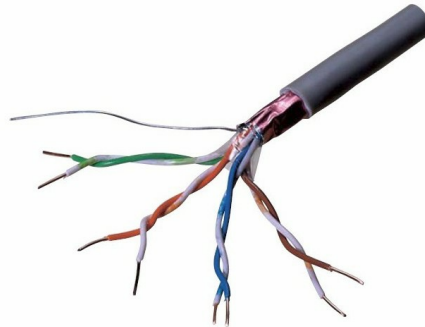
As explained earlier, shielding helps to protect the cable from external signals. As the cable unravels, it acts as an aerial, collecting more external signals as the distance increases. For this reason, we shield the cable from these noises by using two techniques:

- **Shielding:** Here, the whole set of wires is wrapped in foil, which protects it from external signals to some degree. With coaxial cable, this protection is increased as copper braiding is used. A shielded cable comes in one of two forms:
  - Each wire is shielded (or each twist is shielded)
  - The complete set of wires are shielded before the cable is sheathed in plastic. Either way, the intention is to eliminate interference and to minimize crosstalk if possible (the first option will also help to reduce crosstalk, but the second will combat outside interference only).
- **Balancing:** By sending the binary opposite signal across the other wire that makes up the pair and then twisting them, any interference from the binary opposite cancels out interference on the main wire. That way, it is possible to reduce the impact interference will have on the signal.

The different types of twisted pairs available are STP, UTP, Cat3, Cat 5, Cat 5e, Cat 6, Cat 6e, Cat7, plenum, and PVC:

- **Shielded Twisted Pair (STP):** A shielded cable is one that contains further plating or shielding to protect the data signal being sent along the wire from interference (random noise from other equipment, or electromagnetic interference) or from crosstalk (signal bleed from other local data wires).
- **Unshielded Twisted Pair (UTP):** The unshielded cable contains no additional shielding, so external signals will degrade the pure signal, causing alternative data to possibly also be sent on the wire. Crosstalk is removed from the wire only by protecting it from opposing data. The wire is twisted with its opposite, and the data stream is sent on one wire and the opposing binary signal is sent on the other wire twisted with it. This way, any crosstalk would in fact negate the original signal rather than adding additional data to it, and from the deduction of the inverse signal from the original, the original data stream is still received. The process is known as balancing and is also used widely in the broadcast media, specifically in the audio engineering industry. Here, an unbalanced cable such as a phone cable can only run for approximately 1 meter before the cable has also picked up

sufficient interference to interfere with the signal, generating audio hiss. This is because a wire run across a room would act as an aerial as well as transmitting its own signal. The signals it would pick up would interfere with the data signal we are trying to send, which will garble the original signal. Balancing refers to the fact that the pure signal can be retrieved by the device at the other end of the cable.



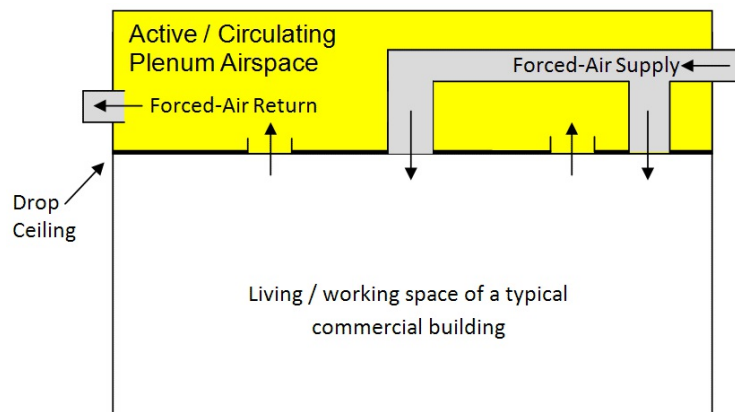
cat5e-shielded-cable

- **Category 3 (Cat 3) cable:** Cat 3 is a common cable designed for short, internal use, for the transmission of telephone signals (voice-grade). It can be used for networking and will transmit up to 10 Mb/s. However, Cat 3 would not be sufficient for modern data networks. Cat 5 is the more common networking cable for internal use and has now superseded Cat 3 as we have now moved to a unified voice and data model over Ethernet.
- **Cat 5:** This is the more common networking cable for internal use. It can transmit 100 Mb/s over 100 meters. Due to high demand, costs are considerably low, so this is the most ubiquitous of cables available on the market. Of the four pairs of copper wire, only two pairs are actually used to send the signal.
- **Cat 5e:** This is a development of the existing Cat 5 cable where all four pairs of wires are used to transmit the signals. Here, speeds of 1000 Mb/s are possible using the existing physical infrastructure. The e refers to enhanced. The cable is also backwards compatible with Cat 5 and Cat 3.
- **Cat 6:** This is the standardized cable for Gigabit Ethernet, allowing typical speeds of 10 Gb/s. The cable twist appears to be much tighter than in Cat 5, and subsequently there is greater reduction of crosstalk allowing for faster transmission speeds. Cat 6 is not widely used within the UK due to the cost, but is the standard

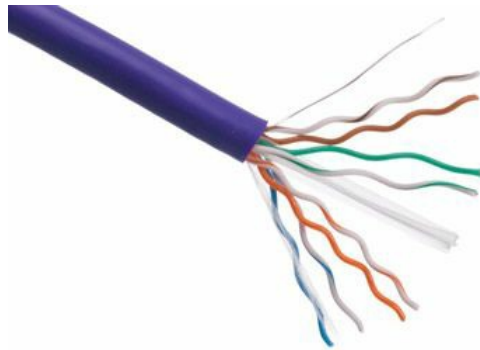
cabling type in the US. The pairs are not themselves coiled around each other but are straight along the run of the cable, forming a body of wiring around a small, flimsy center plastic core. There is a slight barley twist in the center core, but not to the extent of Cat 6e.

- **Cat 6e:** This is a more robust cable. The cable jacket is quite sturdy and its diameter is equivalent to a 25-pair Cat3 type cable, so almost double the diameter compared to the standard Cat 6 UTP cable. Every pair is twisted and coiled around the center plastic core, which itself is barley-twisted to ensure a distance between each pair. The Cat 6e jacket is quite sturdy, made from thick plastic. The jacket also has sections that again separate the four pairs from each other, reducing crosstalk within the cable. The cable is much heavier and is typically used internally when cabling an office to its switch room.
- **Cat 7:** This is relatively new, but it is the common standard for Gigabit Ethernet. Cat 7 is effectively Cat 6 with shielding across each pair and also across the whole cable. In fact, the data transmission on Cat 7 is 10 Gb.
- **Plenum:** I have mentioned this word a few times now. Plenum space is the void space where cables run, either below flooring or above false ceilings in offices. Cables run (splay) on metal trays suspending them across their run. The key here is that there is airflow within that space.

Now, think of possible problems here. In the event of a fire, the airflow moves oxygen around the building, and from this the fire may spread. As the heat increases, the cable wires may act as a fuse, the plastic sheathing (plastic is a fuel) may act as an accelerant, so the fire may spread across the building through the ducting. For this reason, great care is taken to ensure that the room is connected to the air supply and the dead space around this within the void area is not open to receive air from the air supply. This dead air should be oxygen-low, and it is in this area that cables are added:



Plenum-rated cable is typically fire retardant and when burns is non-toxic so as not to harm fire crews. It will have the term plenum written onto the jacket and is typically (for Ethernet) colored purple to identify it as plenum cable (think purple plenum):



Purple plenum cable

- **PVC: Poly-vinyl chloride (PVC)** is toxic and is the chemical the plastic sheathing and jackets comprise. This is toxic when burned, so for safety reasons normal PVC cabling is not used where there may be a risk of fire spreading. It is, however, used for patching (for example, to connect an end device to a wall socket).

### **What could cause an external interference signal?**



Unsupressed motors, power cables, fluorescent lighting

### **For wireless signals, what could cause interference?**

Microwave ovens and cordless phones.

If two cables have to cross, create the smallest touching surface area, that is, cross them at 90-degrees to each other. Power cables are kept separate from data cables. Each have their own holding trough (known as a pan) in the ceiling plenum space.





# Speed and transmission limitations

In this section we will consider connection protocols used across the network, considering their speed and distance limitations.

Protocols: TCP, USB versus Firewire.

With the TCP and USB protocols, the maximum possible transmission speed is not achieved straight away. In the case of USB, the lowest possible speed is reached and each possible transmission speed higher than this is tested in increments until a happy speed is reached, accepted by both end parties. This is done through negotiation along the route (for example, if you have to transfer through a 10 Mb switch then the entire transmission will slow to 10 Mb.). TCP will handshake using the principle of the three-way handshake to establish a connection and agree a common speed.

Firewire, on the other hand, sends at the highest possible transmission rate from the first instance.

If the end device (PC) is also hosting a virtual machine, it too will want to send data, so the data flow may need to be shared across the cable and outwards onto the network as now we have in practice two PCs sharing the same NIC and fighting for its use. This will also impact on data transmission.

Bandwidth is the measure of the amount of data that can be sent across a medium at one time. It can be shared (in the case of the preceding example, the real and virtual machine data can be split by a ratio, or take turns to send and receive their packets.)



# Splitters and effects on signal quality

A good example of this sharing is a phone splitter. On analog domestic phones, an ADSL broadband splitter box was used to connect both the phone line (which used the audible portion of the frequency spectrum) and the higher frequencies for data transfer.

For the musicians in the room, have you ever played a chord? How about the same chord over several octaves? It gives the sound gravitas and is the whole reason why orchestras are made up of instruments that have high and low frequencies. The ADSL limits the frequencies we can use, so as a result the bandwidth is equally limited:

- **Asynchronous Digital Subscriber Line (ADSL)** splits the bandwidth into a send lane and receive lane (known as upstream and downstream). As a home user, how many websites do you manage? Do you send more data than you receive from the internet? No. In fact, it is the other way around - we download a lot more than we send.
- **Synchronous/Symmetric Digital Subscriber Line (SDSL)** is used by professional internet companies, such as web developers who need to regularly upload as much as they download at the same time.

With a splitter, therefore, you are not using the entire frequency range, and as a result speed may be compromised:



ADSL splitter/filter

The other problem if using a splitter is that every phone socket in the house needs a splitter box attached, otherwise the phone using the full bandwidth will create crosstalk and interference leaking over into the higher range used by the ADSL broadband

service, so data transfer will be reduced and packet loss will occur.



# Coaxial

Here are the types of coaxial cable:

- **RG-59** is a coaxial cable used for low-power video signals, such as for CCTV. It consists, as with other coaxial cables, of a solid copper core (75 ohms) surrounded by a plastic insulator, a copper braided wire mesh that shields the inner wire from external interference, and finally an outer plastic jacket. RG-59 is commonly used with broadcast video equipment, but for short range only, such as to connect a satellite dish to the set-top box.

This is comparable to RG-58, which is used for radio and was in use within the early 1990s as Thinnet (10BASE2). RG-59 is not commonly used for networking but is used where broadcast video may need to be transmitted, such as from a security camera to a receiving station before media conversion onto the TCP/IP network. RG-59 carries two wires that can be used to supply power to your external device (for example, your security camera), although it is also possible to use these wires to provide audio:



RG-59 cable

- **RG-6** is a low-loss data cable widely used for short-range connections such as to connect a video recorder to a TV. RG-6 is also 75 ohms but lacks the power wires. The main deciding factors here are install time (do you want to run additional power cables to your external device?) and impedance. If the equipment is designed to run above 50 MHz then you will want to consider RG-59.



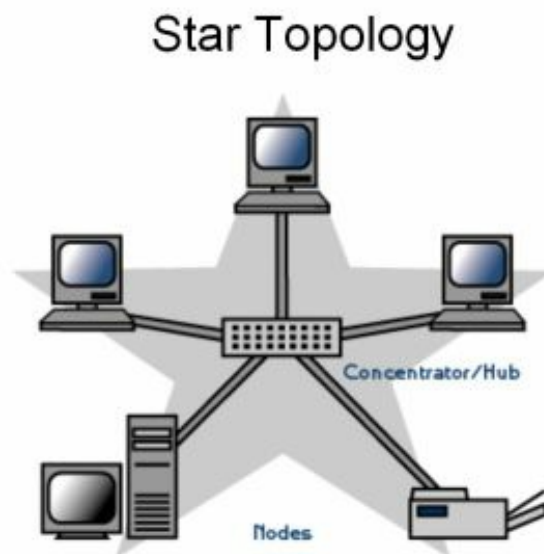
# Speed and transmission limitations

The coaxial cable is more robust than Ethernet and the protective shielding works well to protect from interference. The plastic core protects the thick copper wire, making it a very sturdy and reliable cable. There is, however, only one wire, and resistivity is greater than with Ethernet. The preference is definitely Ethernet for short distances, but coaxial has its uses - it is synonymous with A/V and CCTV equipment usage and can be laid outdoors.

The cable can bend, but is not as flexible as Ethernet. The coaxial cable's distance is up to 500 meters; compare this to Cat 5 cable, which can only run 100 meters. Both can carry the Ethernet protocol signal, so it would be wrong to associate Cat 5 cabling with Ethernet (it is commonly referred to as an Ethernet cable, but this is a misnomer.)

Coaxial cable is also synonymous with early networks, such as IBM's Token Ring. Here, each PC connects to a central hub referred to as a Media Access Unit (MAU). The packet is sent on the network in a ring fashion, from PC to PC from the central hub until the correct PC is identified. In reality, the physical wiring is that of a star network, with the MAU in the middle and each PC as a spoke.

Transmission speeds with Token Ring (as used in the 1990s) were 4 or 16 Mb/s, as opposed to Ethernet, which at the time was 10 Mb/s.



A star network topology



One advantage of coaxial cable is that it is very easy to add a further spoke and PC to an existing cable run. To do this, you switch off the power and cut the cable at the appropriate place with scissors, then fit BNC ends to the cable. The cable is joined together using a t-junction. The other alternative is a t-junction that bites into the cable, referred to as a vampire tap, similar to cheap external garden taps that connect to the existing cold water pipe:



A coaxial vampire tap



# Splitters and the effects on signal quality

The problem with using a coaxial splitter is that the connection is now quite fragile. Any physical movement could dislodge the cable and cut the connectivity for that portion of the network. It is not easy also to find the break in the cable, so a Time Domain Reflectometer is used to measure the time taken to send a test signal along the cable to the point at which the signal stops.

This is then extrapolated into a distance, so that the break can be located.



A Time Domain Reflectometer



# Exam questions

1. Which device is used to check for a break in a coaxial network cable where the break has not yet been discovered?
  1. Multimeter
  2. Optical Time Domain Reflectometer
  3. Time Domain Reflectometer
  4. Butt-sett
2. Which networking topology has a single point of failure?
  1. Bus
  2. Star
  3. Ring
  4. Hybrid
3. Which networking topology uses a common cable shared through all devices and typically terminated at either end?
  1. Bus
  2. Star
  3. Ring
  4. Hybrid
4. For wireless signals what could cause interference?
  1. Microwave ovens
  2. Wired telephones
  3. Televisions
  4. Cordless phones
5. What is the name(s) of the area in an office building used to pass cables from room to room, used due to the lack of recycled air?
  1. Void
  2. Plenum
  3. Cabinet
  4. Cavity



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand and provides an excellent overview and accompaniment to this study guide:

- **Network Cabling (10:11):** <http://www.professormesser.com/free-a-plus-training/220-901/network-cabling-3/>
- **Calculating Signal Loss (4:40):** <http://www.professormesser.com/free-a-plus-training/220-901/calculating-signal-loss/>





## 901.2.3 Explain the properties and characteristics of TCP/IP

So far, we have looked at the physical properties of the network. In this section, we will consider the logical--a numbering system used to identify a specific device on the network that we can configure and control. We will look at the **Internet Protocol (IP)** versions in use today. We will consider the concept of a packet and how this meets OSI layer 3 (network layer). We will consider IP addresses already registered with the **Internet Assigned Numbers Authority (IANA)** and specific reserved addresses we can use within our own (internal, private) network. We will learn of self-configured and emergency IP addresses and how IP addresses can be automatically assigned by a dedicated server on the network, rather than the network administrator setting them manually, or using a mathematical process to carefully manage the IP addresses they have available for them to use.

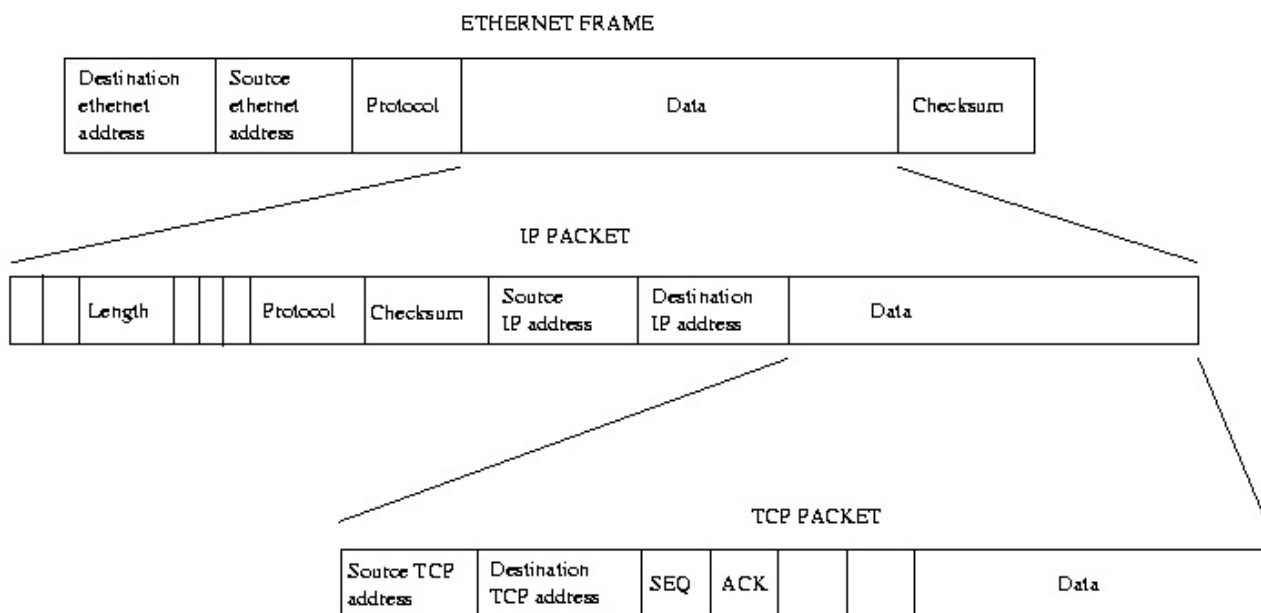
We will learn the required IP addresses needed on the client side for a new PC to not only join the network and communicate on it, but also to know how to find other network resources and a route out of its local area of the network and onto the larger corporate network, even onto the internet.



# IPv4 versus IPv6

IP is a set of instructions that work at the router level (layer 3 of the OSI model). In data terms, the signal sent actually represents a data frame. This contains the payload (the message) wrapped with a header and footer. The header contains information about the type of data frame being sent, its length, where it has come from and where it is going to (both are identified by the MAC address - the physical identification stamp built into the NIC on the PC.) This frame operates at layer 2 OSI.

The data frame also contains additional information that helps it to move across the network and out of the subnet onto the larger network, or onto the public network. Here, routers are important as they act as a bridge or gateway between the different network sections (subnets). Routers operate at layer 3 of the OSI model and read IP addresses to determine where to send the packet, so our data frame now also contains the IP address associated with the MAC address of our NIC at both ends.



Ethernet data frame containing IP and TCP data

When we refer to our data at layer 3 OSI, we are now concerned with the IP address. This is a number we can control. It is a logical number (meaning we can define and change it - it is not tied to the physical device). In fact, IP addresses often change and update as some are only borrowed (leased) for a short amount of time and then released for other PCs, printers, or other network objects to use.

An IP address (IPv4) consists of 32 bits split into 4 x 8 bit portions. As an 8-bit number can be represented as a number between 0 and 255, we write it as a dotted decimal, for example, 192.168.0.1. The four 8-bit sections are referred to as w, x, y, and z. These are denary numbers within each section (an Octet).

With the help of a further number, the subnet mask, we can split the IP address into two pieces of information - the network number (which subnet I am on) and the host number (what is my computer's number on that network).

The IP addresses fall into two categories--the majority of addresses available are in fact purchased from the IANA. These are referred to as public addresses and make up the majority of addresses available. There are, however, reserved sections of the address space for each class where private addresses can be used for internal purposes. These private addresses are not transmitted across the internet but are used within the local site.

An IPv4 address is therefore a 32-bit binary stream that can provide two key pieces of information:

- The network subnet ID
- The host ID on that subnet

This is achieved with an additional piece of information: the subnet mask. A subnet mask is another 32-bit binary stream that is used to separate the IP address into the two pieces of information. After splitting, the remaining information gaps are padded with zeroes. Therefore, 192.168.0.1 can be written as: 1100000.10101000.00000000.00000001.

This is used in conjunction with a subnet mask of 255.255.255.0. This can be written as 11111111.11111111.11111111.00000000.

The process of combining this information uses a logic AND gate where each column provides the A and B input.

An AND gate is a logic gate (an electrical switch) that uses the following rule:

The output is only live (1) when both inputs are also live (1)



INPUT A	INPUT B	OUTPUT C
0	0	0
0	1	0
1	0	0
1	1	1

AND gate and truth table

In our example, we will AND each bit column:

A	192								168								0								1							
B	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1		
C	255								255								255								0							
D	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0		
E	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
F	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1		

AND conversion table



# Legend

- A = IP address (dotted decimal)
- B = IP address (binary)
- C = Subnet mask (dotted decimal)
- D = Subnet mask (binary)
- E = Network ID. This is the AND result.
- F = Host ID. This the IP address with the NID subtracted.

To assist with identifying the classes of an address base on its IP, use the following power table:

$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
128	64	32	16	8	4	2	1

The 'power table' (number base conversion from denary to binary)

Simply add the binary into the columns below one bit at a time and add the numeric values where the column is flagged as 1 together. Thus, 10101000 would be:  $128 + 32 + 8 = 168$ .

To convert from denary to binary, start with the highest number and subtract it from your denary number. If the subtracting number is higher than the number you are trying to convert, then the binary is 0 and you start on the next column across to the right until you are able to find a subtracting number that is lower than the starting number. Subtract the number from your starting number, and any remainder is carried over to be worked on by the next column until zero is reached. This way, you are distributing the number across all columns.

For example, 30 would be distributed as no 128, no 64, no 32, one 16, one 8, one 4, one 2, no 0.

So, 30 is 00011110.

Also, where there is a row of 1s, there is no need to add all of these together to determine your denary equivalent. Simply imagine what the next leftmost column would look like (for example, in the preceding table, column 9 would be 256) and deduct 1.

So, 11111111 would be  $256 - 1 = 255$ .

IPv6 is a relatively new format, but in truth it was introduced publicly by the Internet Engineering Task Force in 1998, although it was not until the wider migration to Windows Vista, which used IPv6 as the default IP addressing scheme, that IPv6 became the standard addressing system.

IPv6 is a larger data packet with a 128-bit addressing system in comparison to IPv4's 32-bit. There was no public release of IPv5; instead, further development led to the eventual release as IPv6.

The main problem we have faced with IPv4 is that we would soon run out of IP addresses. This has now happened. Internet routers tend to support IPv4 as the main common system, although there is an initiative to upgrade the internet to IPv6-capable routers. CompTIA refer to the IPv6 internet, but in truth, IPv4 is still widely used.

IPv4 is still used internally for private addressing as network designers may wish to create subnets of specific sizes and can use now older methods such as CIDR, subnetting, or supernetting to do this. The sheer large number of IP addresses available with IPv6 negate the need to produce a complex subsystem.

IPv6 provides a large address space and advanced protocol headers for the data packet, enabling us to control more advanced packet forwarding. IPv6 nodes can determine their own IP address, simplifying IP configuration. We now use large packets called jumbograms capable of carrying bulk data transfer between ISP provider systems, or across different networks. The packet can be both authenticated and encrypted. The packet can also support QoS labels to identify which data packets are to be prioritized.

IPv6 no longer supports broadcast packets. Instead, we use Multicast (specific PCs) or Anycast (whoever is able to join the data stream).

IPv6's capabilities are further extensible, making it an ideal future technology. On Windows 8.1, IPv6 support is the default addressing system and is enabled by default, but it was optional with Vista and 7. Other technologies, such as IPsec tunneling and DirectAccess, both make use of IPv6. Windows 8.1 secure file sharing and Remote Access Service also now use IPv6.

IPv6 is also capable of Neighbour Discovery. By sending the host MAC address, it can register received solicited MAC addresses from other devices, or IPv6 routers.







# Address structure

For a General Unicast address, the 128-bit IPv6 packet is broken into three parts: a 48-bit routing prefix, a 16-bit subnet ID, and a 64-bit host identifier.

A Link-Local address consists of a 10-bit prefix and 54-bits as zero-padding, with the 64-bit host identifier.

A General multicast would have an 8-bit prefix, a 4-bit flag, a 4-bit scope, and then 112 bits as the group ID.



# Address compression

An example IPv6 address is: 2001:0bc2:25d2:0000:0000:8bbd:0261:6231

Therefore, we can see eight groups of four hexadecimal digits. Each group is separated by a colon.

Where the group starts with a 0, these zeroes can be omitted; for example, 0bc2 can be written as bc2.

Where there are groups of zeroes, the entire section can be removed and replaced with a double colon. This can, however, be done once:

2001:0bc2:25d2:0000:0000:8bbd:0261:6231

This can be written as follows:

2001:bc2:25d2::8bbd:261:6231

IPv6 addresses are recognizable by looking at the first group:

- A network zero IP address with all 128 zero bits refers to an unspecified address (for example, 0000:.....)
- ::/0 refers to the default route.
- ::1/128 refers to the loopback address for NIC 1 on the current host.
- fe80::/10 refers to a local address on the same subnet (link-local). This is the equivalent of a private IPv4 local address (or even **Automatic Private IP Address (APIPA)**).
- fc00::/7 refers to a unique local address between sites that are set to support unique local.
- ::ffff:0:0/96 refers to a 4 to 6 IP address where an IPv4 packet is used on the IPv6 address space.
- 2002::/16 as preceding, this is used for 6to4 translation, where an IPv6 packet is encapsulated into an IPv4 packet to be sent across a portion of the network that supports IPv4 only.
- 2001::/32 is used for Teredo tunneling. This is a Virtual Private Networking protocol requiring access to a Teredo server and Teredo-supporting routers.





# Public versus private versus APIPA/link local

IP addresses are assigned and registered with the IANA (<https://www.iana.org/numbers>). Public addresses are those reserved and purchased for people to use to access the global network. For example, a company would purchase one public IP address to expose its network to the global network. A router is capable of adapting IP packets for use on the global network, referred to as the public network by stripping off the private IP address used for internal, local use and instead adding the public IP address so that traffic will then return to the router, and the router will then know which local resource to send the returning data to.

So as a rule, public IP addresses are registered with IANA and the number is unique. We are running short of IPv4 addresses, so the move to IPv6, where there are millions of IP numbers available, has helped the internet to expand as every device used needs an IP address to connect to the cloud and the wider global network. Even fridges and other home devices can now connect to the internet in what is called the **Internet of Things**.

However, certain IP numbers have been deliberately reserved for internal use, or for testing, or other purposes. These are referred to as private addresses. The following table lists the table and approximate information to recall private IPs for the first three classes:

A	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.255.255
C	192.168.0.0 - 192.168.255.255

Standard classful addresses

Although there are private address regions for all classes defined by IANA, only the preceding ones are commonly used.

Class D addresses are specifically used for multicasting, for example, video conferencing. Class E and F are used by research, government, and military establishments, and their use is out of the scope of this course.

Addresses ending with .0 infer no host on this subnet and therefore are simply



describing the subnet.

.255 are broadcast addresses - a shout-out to all nodes within the same network. The DHCP process is an example of where broadcasts are used. Also, internal routers would need to be able to route broadcasts (referred to as BOOTP requests) for the process of imaging and deployment, as the initial stage of imaging a blank PC is to boot across the network from the PXE-enabled network card (NIC).

**Automatic Private IP Address** translation (commonly referred to as **APIPA**), also referred to as Zero Configuration Networking, was designed originally to circumvent the need for manual IP configuration on a corporate subnet (link-local). The operating system (in this case, Windows 2000 and above) will auto-assign an address in the range 169.254.x.x, where x is a randomly generated number between 0 and 255 (not inclusive, as these are reserved) in the hope that other local clients on the same subnet will do the same, allowing the PCs to connect.

APIPA link-local addresses are non-routable and as most corporate networks rely heavily on the DHCP service, it now infers a wider problem with the DHCP server, or that the router connecting the subnet to its DHCP server is now not broadcasting DHCP heartbeats. Assuming that network connection to the DHCP server is good, and that the DHCP server is authorized and active, the process of IPCONFIG/RENEW will release the APIPA address and the service will be re-established. This is usually an automatic process - there is no need to manually force a renewal, and the DHCP server will have broadcasted to the subnet typically within 10 minutes, so if several PCs are affected, patience is all that will be required.

APIPA addresses always start with the numbering 169.254.x.x.

Loopback--127.x.x.x is used for testing. It is not strictly a part of the A or B classes as it cannot be configured and used to define a device on the network. If I send a test packet on the local machine using 127.0.0.1 I am asking to send the packet on the first NIC physically installed on this local machine. This is referred to as the loopback address.

The `PING` loopback command works because the operating system contains a system-managed text file called a Hosts file, which stores hard-wired IP addresses and their associated computer name. Loopback is part of the hosts file by default.



# Static versus dynamic

If the IP address has been manually assigned (that is, you have added it to the NIC manually with a PowerShell or NET command, or through the GUI) then it is said to be static. It will not change and other network resources will always use this number.

The analogy is like a mobile phone contract, where the phone number is analogous to your IP address. The mobile phone number was set when you signed the contract and will not change.

Certain devices have to have their IP address set manually, such as old network-enabled photocopiers where the IP address is added to the firmware on the machine itself.

Most end devices, such as tablets, laptops, or PCs, actually auto-configure. They receive their IP address after a conversation with the DHCP server - a dedicated server that issues IP addresses across the network. The DHCP server manages a range of IP addresses and logs that are active. Typically, a dynamically-assigned IP address is leased for eight days (wired) or one hour (wireless), but this can be changed on the server when the scope is first set.

It is good practice for key servers on the network, such as the DHCP, DNS, and Domain Controller should be static because dynamic addresses may change - the device might receive a different IP address depending on the availability of IP addresses within the given range (the scope).

If two devices have the same IP address, for example, one is assigned statically and one is dynamic, the dynamic device should drop out of scope, meaning that the IP address will reset to 0.0.0.0, meaning I'm not on the network right now - there is a problem. To resolve this, either set an exclusion in the scope (if the static IP is correct), or correct the misconfigured static IP.



# Client-side DNS settings

This is all fine, but users do not go around remembering IP addresses. Using the phone analogy, we might remember a few phone numbers but we have a phonebook (contacts list) on our phone for that. You register the person's name and their phone number just like this on the PC; when we connect to another computer on the network, we usually do so by name.

So how does the PC translate and find the IP address? A DNS query is sent to the local DNS server. This is a database containing a list of IP addresses and their associated computer name. The query is by way of a Forward Lookup, meaning that the name will be looked for and if there is an address record the IP address associated to that name will be returned. Your end device will then store this IP address for later use and whenever you reference a device by name, the IP address is now already known and stored in the local cache, so you can send packets directly to it.



# Client-side DHCP

By typing `IPCONFIG /ALL` (`IFCONIG` on Linux/Unix systems) you will receive a list of the current configuration, but it will also state if the IP address was assigned by DHCP. Wherever possible, if the lease expires DHCP will try to issue the same IP back to the end device, and for this to happen the end device regularly contacts the DHCP server to remind it how far through the lease the end device is.





# Subnet mask versus CIDR

As mentioned earlier, the subnet mask is used to split an IP address into two portions - the network ID and the host ID. Classful addresses have a subnet mask in multiples of 8 bits:

- Class A is 255.0.0.0
- Class B is 255.255.0.0
- Class C is 255.255.255.0

**Classless Internet Domain Routing (CIDR)** is a technique used to explicitly define and describe a more tightly managed subnet, and by so doing you can reduce the number of IP addresses defined within the subnet. A CIDR address is usually written with a suffix that denotes the number of bits used to describe the network portion of the IP address. On a standard classful system we use blocks of 8 bits to define the standard classes, A, B, and C, like this:

- 0.0.1 / 8 defines 255.0.0.0 as the subnet mask
- 172.16.10.1 /16 defines 255.255.0.0 as the subnet mask
- 192.168.1.10 /24 defines 255.255.255.0 as the subnet mask

With a CIDR notation, the number of bits used does not fall into this common pattern. We have borrowed a bit to be able to double the effective number of PCs within the subnet, but by doing so we have halved the amount of subnet networks available.

It is also important to note that on a CIDR system the starting IP address numbers used give us our starting position. Usually, therefore, a 192 address started out life as a class C, so if the suffix is /22 this infers that 2 bits have been borrowed. However, there is no real correlation between the numbers used and the suffix.

When we are describing a subnet mask by its bit length we use the term **Variable Length Subnet Mask (VLSM)**. Each section can be carved up into areas of differing lengths until the space available is used up.

In the example 192.168.1.10/22 we are borrowing 2 bits from the network portion and will quadruple the number of available PCs within our network.

The formula to calculate the number of hosts is  $2^{(32-n)} - 2$

Here,  $n$  is the number of bits as defined by the suffix. In the preceding case,  $n = 10$ .

Therefore,  $2^{(10)-2} = 1,022$  hosts within each subnet.

In this example, the number of subnets that can be created with a /22 CIDR mask is 4,194,304 subnets. This is using the equation  $2^n$ .

The first block IP range would be: 192.168.0.1 to 192.168.3.254.

In reality, the propensity of IPv6 addresses makes CIDR redundant, but still expect to see this as a job interview question! This is a good discipline to learn and may help you if you have to be responsible for every IP address issued. A good example might be a web hosting company. It has a range of public IP addresses and companies pay to host their websites with them using a shared server. Each company needs one or several IP addresses from the range, so these are loaned as part of the hosting contract.

CompTIA regularly state that they will be dropping CIDR from the exam, but with each version it is still there. Expect to know how to perform a CIDR calculation - it will be worth a few easy points in the exam.



# Gateway

Look around you. I am assuming that you are in a room and nearby there is a doorway. The doorway has two handles - one on either side of the door. This is analogous to a router, which connects portions of the local physical network, referred to as subnets, together. Each subnet is defined with a different network ID (for example, `192.168.1.0` for subnet A and `192.168.2.0` for subnet B). The router keeps a routing table defining each subnet and which physical port and network cable to use to communicate with each subnet (for example, subnet B may be on port 5). The formal term for a router acting as a connection point between two or more logical networks is a gateway.

In order for the end device to function on a network, it needs to know the following:

- What is its unique identifying number?
- What subnet is it on currently?
- How do I find out about other devices on the network, both in the subnet and across the wider network?
- How do I get out of the subnet?

For this, you enter the following information:

- IP address (static or dynamically assigned)
- Subnet mask
- DNS server IP address (if dynamically assigned then this can also be retrieved from the DHCP server when the IP address lease starts with extra information known as Scope Options)
- The router's IP address on your local subnet



# Exam questions

1. What is the specific purpose of a gateway?
  1. To send data outside of your area of the network
  2. To access the internet
  3. To communicate to a neighboring PC
  4. To send images via Bluetooth
2. In CIDR, a subnet of 23 bits will provide how many hosts?
  1. 254
  2. 126
  3. 62
  4. 510
3. Which IP class is used for video conferences and Skype calls?
  1. A
  2. B
  3. C
  4. D
  5. E
  6. F
4. What is the purpose of loopback?
  1. To check that the network card is able to transmit and receive
  2. For the device to send data back to itself
  3. To communicate with another PC on the network
  4. To listen for incoming data signals
5. Your PC receives an APIPA address (169.254.10.23). What wider problem does this indicate on the Enterprise network?
  1. The DHCP server cannot be reached
  2. The DNS server cannot be reached
  3. The switch is misconfigured
  4. The firewall is misconfigured



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand and provides an excellent overview and accompaniment to this study guide:

- **An Overview of IPv4 and IPv6 (11:56):** <http://www.professormesser.com/free-a-plus-training/220-901/an-overview-of-ipv4-and-ipv6-3/>
- **TCP/IP Addressing (6:48):** <http://www.professormesser.com/free-a-plus-training/220-901/tcpip-addressing-2/>





## **901.2.4 Explain common TCP and UDP ports, protocols, and their purpose**

Moving on to OSI layer 4 (transport) we consider numbering used on firewalls to define the type of data we are sending. We can filter based on this data, limiting certain services access through security boundaries and thereby protecting our resources.

In this section, we will also list some of the standard basic network services you will use on an enterprise network.

Finally, returning to the firewall, we contract the two transport protocols used to send files and to stream data (for example, video conferencing).



# Ports

At OSI layer 4, firewalls are used to stop traffic from entering or leaving the network. The port number refers to a number used and added to the packet to identify the data's use and purpose (for example, HTTP web traffic uses port <sub>80</sub>).

Here is a list of common ports that are globally recognized. Remember you can use different ones but the convention is to use these numbers:

- **20, 21 FTP** is used in the connection to a public FTP site in order to download files, a website, or a Git repository. In itself, FTP is not secure, but additional security connections are available to secure connection (authentication) or to encrypt the data stream. We no longer use 20 to receive data, but instead on 21 the handshake to the FTP server allows the firewall to open a dynamic port (that is, one only open for the life of the connection to the server and closed when the communication is concluded). This dynamic port is randomly assigned but is a high number not commonly used or associated with any other service.
- **22 SSH** (Secure Shell) is used to create a secure connection between endpoints. It is commonly used with OpenSSL/PuTTY or Remote Desktop to establish and to maintain the connection between the connecting and target machines. As well as remembering 22, also associate this number with port <sub>3389</sub>. Together, they form the handshake and the data stream of the remote connection.
- **23 Telnet** is an older but popular management system. This is used to send remote commands from a client PC to a target PC. However, you need to authenticate to the target PC, so you need to present the username and password of an account that will be accepted by the target PC. However, all information is sent between the two PCs in the clear. Telnet is not an encrypted channel.



**WARNING:** Do not use Telnet. Port <sub>23</sub> is not encrypted.

- **25 SMTP** the Simple Mail Transfer Protocol is designed to send emails from an email server to either the recipient's mail server, or to another email server within the company (for example, if the branch office mail server sends all outgoing mail to the head office's mail server where they are compiled, virus-checked and compliance-checked before sending the mail outside of the company network). Both SMTP and POP3 are old technologies but are still widely used. POP3 is

being phased out on newer Microsoft Exchange servers, favoring IMAP instead. However, it is good to memorize SMTP and POP3 together.

- **53 DNS** (Domain Name System) is used to send DNS requests and resolves between the client and DNS server. DNS resolves name requests to IP addresses to inform the client the specific IP address to use to then forward communication directly to the computer by its IP address. DNS servers can also forward requests onto either other internal DNS servers, or to the internet root servers (referred to as root hints). The edge server on a network is set up to communicate to the internet to the Internet Root servers. Within the network we use local DNS servers which will forward requests on to the edge server. Each DNS server involved may host their own list of zones so internal resources can be found before the query otherwise will be sent out to the internet.
- **67,68 DHCP** (Dynamic Host Configuration Protocol) DHCP in this context refers to the DORA (Discover, Offer, Request, Acknowledge) process where broadcasts and unicasts are used to request a new client IP address, also to locate a DHCP sever on the network. Not only is a client IP lease provided but also a series of other significant IP addresses that may be useful to the client. These signpost IP addresses may identify other key network components such as the location of DNS servers, Default Gateways (routers), IIS (web servers) and other services. Upon second presentation of the client onto the network, the final two stages are used (RA) as the DHCP IP address is already known to the client.  
It's not in the original list or in the exam, but it is worth noting the DHCP ports when you are imaging a PC across the network (a typical first-line and second-line support task).
- **80 HTTP** Hypertext Transfer Protocol. This replaces Gopher and Finger protocols and is used for all internet traffic, for example, web pages. Data is not encrypted if you are using port 80.
- **110 POP3** Post Office Protocol v3. This is an old protocol associated with receiving emails on mail servers. This is associated with SMTP, used to send emails.
- **143 IMAP** The Internet Message Access Protocol is used for web access to email, such as via Yahoo or Hotmail. Emails reside on the web-based email server and you view them remotely using a web page, whereas with POP3 the message is actually sent and stored on the local PC.
- **443 HTTPS** Hypertext Transfer Protocol Secure. This is also known as HTTP over **Transport Layer Security (TLS)** and also HTTP over Secure Sockets Layer (SSL). This depends on the version of encryption being used. As with port 80 this is used for web traffic, especially for web-based email. The advantage is that the

data is sent in an encrypted format, typically using a certificate file installed on both the client and the server (both ends of the connection).

- **3389 RDP** Remote Desktop Protocol. This is used in conjunction with port 22 to send the data of a remote connection session when connecting to another PC across the network.



Remote Desktop to Windows 10 from Apple PC.

- **137-139 NETBIOS**. The NETBIOS protocol is an extremely old protocol used to query computer names and to find their IP addresses. It was used up to and including Windows 95 but has long since been superseded by DNS. As a result of this we usually leave these ports closed.
- **445 SMB** Server Message Block is an important protocol that provides network shared access to files and printers. It is considered to be an inter-process communication system in that it is controlled by the operating system and defines how and which parts of files to send from one PC to another. We often consider the fact that file data is stored on a hard drive as blocks, and that data is transferred as a low-level system; however, in reality the operating system takes the responsibility of managing the transfer. SAMBA is one implementation of SMB used on typical systems specifically for file transfer through the internal network
- **427 SLP** Service Location Protocol. This port is used to find information about

computers and other devices on the local network that have not yet been configured and installed onto the operating system. For example, if you add a new network printer, SLP is used to discover the device that will then prompt the operating system to install the printer. SLP uses agents - software modules. A User Agent is a device that can search for new services on the network (that is, the end user's PC can locate other devices). A Service Agent is the opposite of this - the printer would broadcast on the network to say that it is available for others to find. Directory Agents (for example, the Active Directory database on the Domain Controller) will then list the object in the directory making it easier for others to find the device, especially those where SLP is not enabled on the network. On Apple systems, SLP was an easy way to discover printers newly added to the network.

- **548 AFP** Apple Filing Protocol (AFP). Either port 427 or 548 can be used to transfer files using AFP instead of SMB. Usually it connects to an Apple file server, but with Mac OS X v10.4 peer file transfers can take place, eliminating the need for an Apple file server.





# Protocols

This next section will focus on network services and communication languages specific to services across the network.



# DHCP

The Dynamic Host Configuration Protocol (DHCP) is an important server service offered across the network. As a concept it is fundamental to the A+ course.

A DHCP server will listen for any broadcast packets from no registered PCs. A DHCP server is designed to lease out IP addresses to devices as they need it. Typically, a device keeps the IP address for 8 days, after which time a request for another 8 days is made.

There are four stages to the DHCP lease:

- **Discover:** A broadcast packet is sent from the new requesting PC across the network. The DHCP hears this packet and the DHCP process starts.
- **Offer:** The DHCP server checks its cache of available IP addresses. If there are sufficient IP addresses available within the range (the scope), then an IP address is offered.
- **Request:** The PC requests to use the IP address it has been offered.
- **Acknowledge:** An acknowledgement packet is sent to the PC, which then starts to use the IP address. It is at this point that the lease starts.

An image that may help you to remember the mnemonic is the children's TV series Dora the Explorer. Visual mnemonics aid memory retention. By the way, routers send DHCP messages using the same ports as are also used when taking an image across the network, using the BOOTP protocol. In Nickelodeon's Dora the Explorer, Dora's companion is a monkey called Boots! How coincidental.

When the IP address is issued to the PC, other information can also be provided, in fact DHCP will act as a gateway to other important services and network locations:

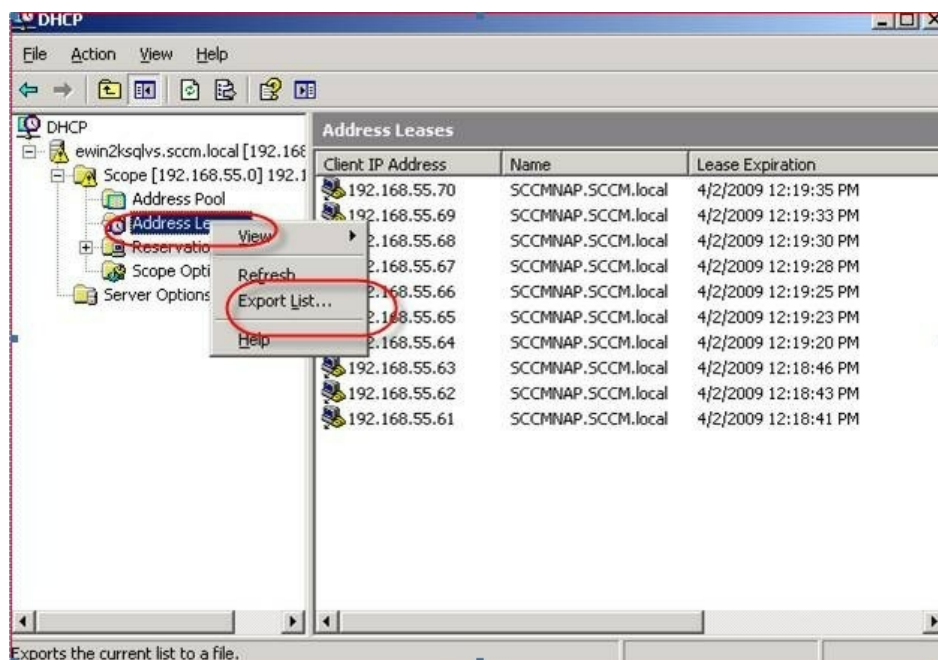
- The router default gateway IP address
- Location of the DNS server
- Location of the IIS web server
- Local printer IP addresses for this subnet

It is up to you as a network designer to determine if you want to issue information to your clients through DNS, or through DHCP. Usually it is common to signpost services (for example, IIS and printers) through DNS but to place the location of the DNS server

as a DHCP signpost, without which the new PC will be unable to locate network resources.

When setting up a DHCP scope, it is important to remember that the scope is a logical set of IP addresses, but physically it is likely that the devices will be local to each other, within the same building, floor, or even room. They exist as part of the same subnet and will probably be connected to each other via a switch. They will access the rest of the network outside of their subnet via a router. This poses a problem - by default, routers block broadcast traffic, as is detailed in RFC 1542. Effectively, routers block broadcasts. As the initial stage of the DHCP process involves the DHCP server hearing a broadcast on the subnet, the DHCP server would be unable to service requests on the same subnet if a router was stopping broadcast traffic. It is quite sensible for routers to block broadcasts - without this, a network storm would be created as your new PC attempts to ask the entire internet for the location of a helpful DHCP server.

The DHCP service is significant on the network, so it is the role of the network architect or manager to approve any new scopes added to the network. Your network might have several DHCP servers, or one for every subnet on the network, or possibly one at each branch of your organization. To avoid conflicts, the scopes have to be checked, the scope activated, and the DHCP server authorized before DHCP will start to issue new IP addresses.



DHCP scope





# DNS

**Domain Name System (DNS)** is a service that is usually dedicated on a server that is capable of serving requests across a portion of the network. The DNS server regularly receives information from devices, acting as a kind of phonebook to the devices, offering lookups or resolutions and helping the PC to find where a network resource is located. DNS is at the top-most level of the directory services model:

- **DNS:** A lookup service that translates name requests to resources or other devices to their IP address
- **DHCP:** The service that issues an IP address to a MAC address
- **ARP/RARP (Address Resolution Protocol):** A local table or cache stored on each PC that describes which IP address is used by known local MAC addresses

DNS is a database of known resources referred to as a zone. Different domains can each be services within one DNS server.

A request can be of one of two types:

- **Forward lookup:** This is a resolution from name to IP. This is the most common form of lookup used across a network to find where resources are located.
- **Reverse lookup:** These are not common, and on an internal network there is no need to set up a reverse lookup zone. These are typically used for web servers where the IP address is known and we want to determine on which web server (from many in a cluster) a particular website is located.

Within the zone there are a number of different record types:

- **SOA:** The Start Of Authority. It may be possible that you have many DNS servers located within your network. Which one should a newly joined PC start with? The SOA denotes the starting point for any new device - this is the primary DNS server within the network.
- **SRV:** The service record denotes key services within the network; usually, these tend to be DNS servers. Other information stored within the record would be the protocol type and port used to communicate with this service.
- **A:** An IPv4 address of a device on the network. The name and IP address are stored.
- **AAAA:** An IPv6 address of a device on the network. The name and IP address are

stored. MX is the location of the Mail Exchange server

- **CNAME:** Canonical name (or alias). By setting a CNAME, another alias can be used to refer to known device on the network. This can make it easier for network administrators to refer to resources and devices by using non-technical names or nicknames to access a particular server. Where a CNAME is known by the client PC, it will then continue to use the CNAME rather than the actual name for the device it is trying to communicate with.
- **LOC:** A location record is used to specify the geographical location record for a device. This is useful if you have different branches located in different cities and want a way of geographically grouping resources.

The process of querying a resource by name in order to find its IP address is called a Forward Lookup. On a local network, it is common only to use Forward Lookups. Reverse Lookups are used typically on web server clusters to determine which actual server you have connected to, if accessing the resource using a common IP.

- **PTR:** Used on reverse lookups, the PTR or pointer refers back to the name. Resolution is the opposite of a forward lookup, this time the IP address is resolved to the device's known name.

The screenshot shows the DNS Management console window titled "dnsmgmt - [DNS\BOALSBURG\Forward Lookup Zones\blackberry.local]". The address bar displays "192.168.251.1". The left pane shows a tree view of the DNS hierarchy under "BOALSBURG", with "Forward Lookup Zones" expanded and "blackberry.local" selected. The right pane shows the "blackberry.local" zone with 11 records. The records are listed in a table with columns "Name", "Type", and "Data".

Name	Type	Data
_msdcs		
_sites		
_tcp		
_udp		
DomainDnsZones		
ForestDnsZones		
(same as parent folder)	Start of Authority (SOA)	[3529], boalsburg.blackberry.local., hostmaster.
(same as parent folder)	Name Server (NS)	boalsburg.blackberry.local.
(same as parent folder)	Host (A)	192.168.251.1
boalsburg	Host (A)	192.168.251.1
Villegas	Host (A)	192.168.251.127

DNS configuration showing Zones with their Forward Lookup records



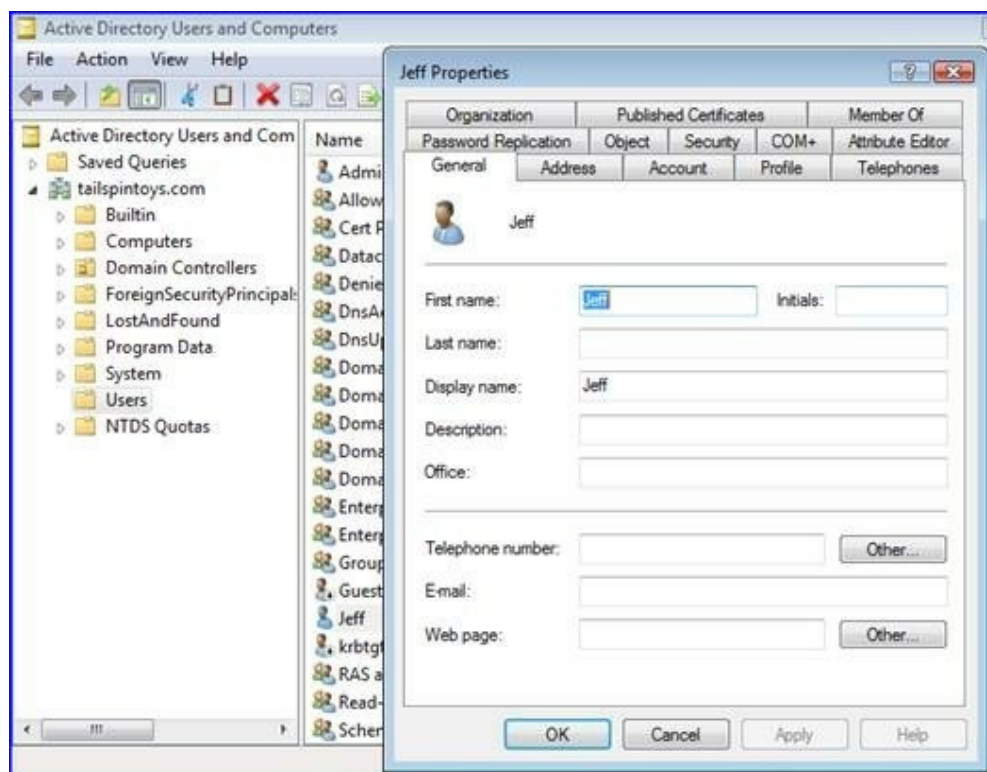




# LDAP

On Microsoft Systems Active Directory (AD. SAMBA on Linux) is a database of user, computer, and printer objects that make up the logical domain. For a computer to connect on the network it must be registered and an object for it created in AD. When the end user PC boots up it communicates across the network to identify itself with AD. AD forms a key part of the AAA security architecture - Authentication, Authorization, and Auditing.

AD objects can be created, modified, or deleted using either the AD GUI referred to as Active Directory Users and Computers (ADUC), or by using console commands. In reality, when ADUC is used Lightweight Directory Access Protocol (LDAP) commands are generated to manipulate the database.



Active Directory Users and Computers

Here's an example LDAP command to add a user:

```
dsadd user "cn=John Smith,ou=SouthEmployees, dc=northwindtraders,dc=com" -disabled no -pwd C^h3E  
-musthpwd yes
```





# SNMP

**Simple Network Management Protocol (SNMP v1 or v2)** is used to send management data to other routers and managed switches. The SNMP suite supports a range of hardware, including servers. Version 3 is secure, so this is now used. The earlier versions (v1 and v2) do not encrypt the data sent.

SNMP is used to check for connectivity, system health or to forward configuration information. SNMP is an accepted protocol amongst NICs, switches, and routers. SNMP spans the whole OSI suite, including commands at the application level. Servers can use SNMP to report their status to a waiting collection point (for example, a client PC).



# SMB

**Server Message Block (SMB)** is an important protocol provides network shared access to files and printers. It is considered to be an inter-process communication system, in that is it controlled by the operating system and defines how and which parts of files to send from one PC to another. We often consider the fact that file data is stored on a hard drive as blocks, and that data is transferred as a low-level system; however, in reality the operating system takes the responsibility of managing the transfer. SAMBA is one implementation of SMB used on typical systems specifically for file transfer through the internal network. This means that file transfer such as copying from one disk to another can be performed extremely quickly with no additional processing required - simply select the blocks that make up the file and copy these. This is also referred to as a low-level copy.





# CIFS

The **Common Internet File System (CIFS)** is an accepted standard for file sharing across the domain, but also across the internet. It is an advanced version of SMB and has been in operation since Windows 2000 server.

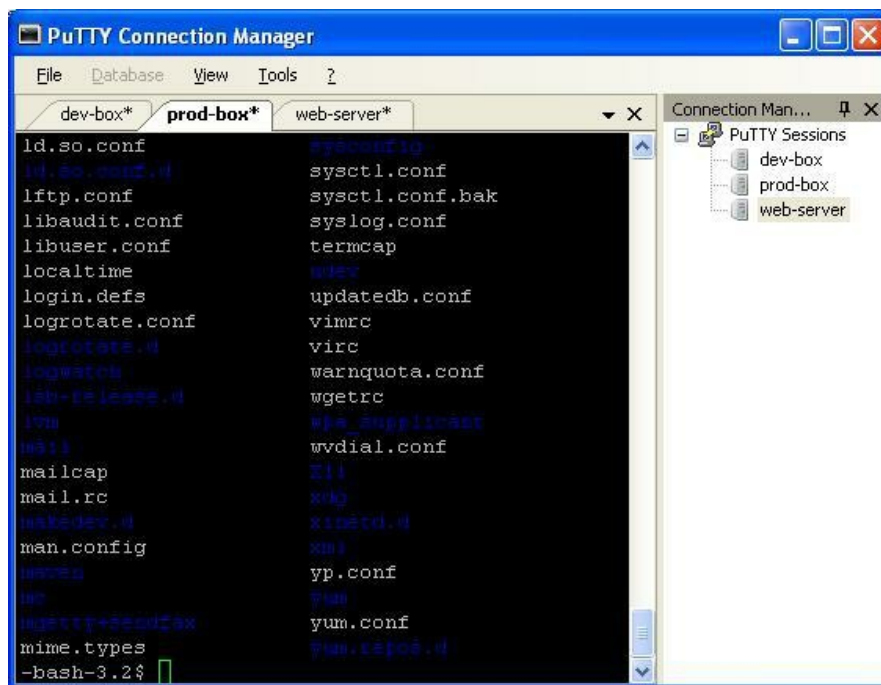
CIFS is in fact a series of commands used to pass information between networked computers. A redirector can send CIFS requests meant for remote computers. The redirector creates a series of connection messages to start the sharing session, mapping a route through the network to the remote PC. Namespace and file change messages are then used to read and write to the server. For internet printing, the redirector can manage the flow of the print queue and also send management and status information about the print queue. For email, the redirector creates a pipe (a dedicated connection) to be able to then send the mail message.

CIFS is standard across a variety of operating systems, including UNIX, IBM servers, and all Microsoft systems.



# SSH

Secure Shell is used to create a secure connection between endpoints. It is commonly used with OpenSSL/PuTTY or Remote Desktop to establish and to maintain the connection between the connecting and target machines. Example SSH applications as Microsoft Terminal Services Client (known as Remote Desktop), or PuTTY, which uses OpenSSH:



A PuTTY session



# AFP

The **Apple Filing Protocol** is a set of commands used on the Apple operating system to communicate with a file server in order to send and receive files. This is an alternative to SMB, which is also supported on Apple systems. Usually it connects to an Apple file server, but with Mac OS X v10.4 peer file transfers can take place, eliminating the need for an Apple file server.



# TCP versus UDP

At OSI layer 4 we define what type of data we are sending across the network.

Firewalls have doorways called ports that are opened as needed to let data through. The port number therefore describes the data and the service that uses it:

- **Transport Communication Protocol:** TCP is used to ensure that data sent is received correctly and is said therefore to be a reliable protocol. With TCP, the two PCs will first attempt to handshake, that is, to establish communication before any data is sent. If a packet receipt is not received in good time, then the packet is resent. Therefore, the receiving PC can maintain and check the packets as they are received until the file is re-structured. There is also a degree of error-checking taking place, which ensures the validity of the data received. TCP is therefore a very reliable protocol making it good for file transfers.
- **User Datagram Protocol:** UDP is not a connection-oriented protocol. Here, a stream of data is sent. There may be errors in the data stream and there is no consideration as to if the data is being received or not. As there is no error-checking mechanism built into the packet, the packet can contain slightly more data, making receipt a little faster, but the data stream will be prone to errors. This, however, makes it a good protocol to use for video conferencing, online video streaming, and webcam streams where the end user will not be too concerned if there is a slight glitch, or where the user may want to opt in or out of a video conference.

There are 1,024 system ports (from 0 to 1023), which are known as the commonly known ports. Preceding this, 1024 to 49151 are the registered ports. They are registered with IANA.

The number range from 49152-65535 are ephemeral ports used for temporary access. These are not used by IANA but are used internally within the network. For example, to transfer a file from PC to PC using FTP you could assign a rule to use Dynamic FTP. Here, port 21 would be used to establish the connection but for security reasons, rather than use port 20 to transfer the data, another dynamically assigned port is used by both PCs.

A port is simply a doorway. Traffic can flow in or out of the port and the port can be set to allow one or two-way traffic. There are 0-65535 ports for TCP and another 0-65535 set of ports for UDP.



It is possible to use any port number, but the port being used must be open at the firewall and known to be used for that specific purpose by both PCs involved. As we are often dealing with public networks there has to be a common standard so that everyone uses the same port for the same purpose.

TCP is used for file sharing as you need an accurate copy of the file to be received. UDP just sends the data and doesn't really care about if there is a glitch or not (think Vimeo, or YouTube video).



# Exam questions

1. Which ports are used for internal email where the email is sent directly to your local PC?
  - Answer:
2. Which firewall protocol stack is considered to be a connection-oriented protocol and is said to be a reliable protocol?
  - Answer:
3. Which ports are used in a Remote Desktop connection (for example, PuTTY)?
  - Answer:
4. Which protocol is used to send configuration, reporting or reboot commands to another router or firewall on the network?
  - Answer:
5. What is the purpose of a DNS zone?
  - Answer:



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand and provides an excellent overview and accompaniment to this study guide.

- **Common TCP and UDP Ports (11:26):** <http://www.professormesser.com/free-a-plus-training/220-901/common-tcp-and-udp-ports-4/>
- **Common Network Protocols (8:00):** <http://www.professormesser.com/free-a-plus-training/220-901/common-network-protocols-2/>



## 901.2.5 Compare and contrast various Wi-Fi networking standards and encryption types

To ensure consistency across the globe, Wi-Fi transmissions comply to **International Electrical Engineer standards (the IEEE standards)**. These define the speeds achievable, distances reachable, and specific frequencies used by each 802.11 standard. We will in this book focus on the common standards: a/b/g/n and ac.

Over these standards we can encrypt a packet to ensure that any information contained in its payload cannot be intercepted and used by a third party. We will look at authentication, protecting passwords, and ensuring the end-to-end connection is secure, as well as different methods we can use to encrypt the packet.

Finally, we will end with the Advanced Encryption Standard - an extension to previous encryption standards that allows us to use ID cards or biometrics so that there are in fact two forms of identification needed for you to access your account (multi-factor authentication).





# Standards

In this section we are going to focus on wireless standards. Focus on distance, frequency and data speed.



# 802.11 (a/b/g/n/ac)

There are several wireless standards currently in use. This section will consider situations where these may be used:

- **802.11a:** This standard is capable of transmitting at 54 Mb/s, which is an advantage over 802.11b. It is, however, prone to physical obstructions and may require expensive professional equipment. Its use of the higher 5 GHz frequency reduces the range somewhat, and so more access points are needed than with other Wi-Fi standards.
- **802.11b:** This standard is capable of transmitting at 11 Mb/s but over considerably longer distances. It is also more reliable than 802.11a in that it is not as easily affected by physical obstructions. It has been available for home networking from 1999. Transmission is at 2.4 GHz, which does make it prone to radio interference such as from cordless phones, baby monitors, or microwave ovens.
- **802.11g:** This standard has replaced the earlier models. It is highly secure and backwards compatible with 802.11b and has become the main standard for computing networking both at home and for the corporate environment. It continues to use 2.4 GHz but allows 54 Mb/s over this frequency.
- **802.11n:** This standard uses a stereo MIMO signal through a pair (or several pairs) of antennae, allowing for triangulation of signal and higher speeds. It was first introduced in 2009 and is now the standard communications type for Wi-Fi routers. It can operate on either the 5 or 2.4 GHz frequencies. 802.11n can achieve a typical 70 Mb/s and a maximum of 150 Mb/s given no radio interference. 802.11n is susceptible to Bluetooth interference, if there are Bluetooth devices within range. It is backwards compatible with a, b and g.
- **802.11ac:** This is a new standard that introduces data transmission rates of 1 Gb/s on a wireless LAN and 500 Mb/s on a single link. This may negate the need for wired connections for corporate or home networks, moving forward. It is based on the same MIMO technology used in n with a wide RF bandwidth, eight MIMO streams, downlink multi-user MIMO for up to four clients and high-density modulation. By combining these tremendously fast data streams with USB v3, it will be possible to have completely wireless cloud solutions or video servers streaming HD-TV signals to fourth generation phones.



# Speeds, distances, and frequencies:

802.11 Wireless Standards					
IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

802.11 Wireless Standards table



# Encryption types

In this section we will look at wireless encryption and password authentication protocols used to protect Wi-Fi traffic.

- WEP is used to provide a cypher encryption of wireless data packets by the use of an encryption key. On its own, WEP is relatively insecure and can be cracked quite easily (referred to as aircracking). Once the key has been determined by a hacker, the entire system is open to attack. WEP is the initial choice available on all wireless routers. WEP is commonly used in either infrastructure mode (for use on domains), or for ad hoc mode (used when two laptops, or smartphones directly connect as a PAN style network).
- WPA can be added to provide an additional layer of security to an existing WEP system. WPA1 was intended to be an intermediate step.
- WPA2 supports AES encryption - this is a very strong encryption standard used on a corporate domain. WPA2 with AES is the de facto standard and the most secure option we have.

In WPA2, Personal mode is used for home and small business (SOHO) networks.

We use a standard password set on both the wireless router and client. WPA2

Enterprise mode makes use of a **RADIUS** authentication server, using the username and password as it appears on the Active Directory database. WPA2 Enterprise is known as **802.1x** and is typically certificate-based. To support WPA, Temporal Key security (**TKIP**), as discussed earlier, will encrypt the data packet using a timestamp. However, if the base time is known across the network, an attacker may be able to emulate the time within the augmented packet they attempt to send.

- AES, the Advanced Encryption Standard uses a cipher known as **Rijndael** (after the names of the standard authors. It is pronounced Rhine-Dale). It is a symmetric key algorithm - the same key is used for encrypting and decrypting the packet. The ciphering process undertakes 10 to 14 rounds in which the packet is augmented by the cipher. AES has the approval of the US government through the National Security Agency (NSA). It is considered stronger than 3DES (known as Triple DES), which is a three-round cryptographic process.





# Exam questions

1. Which data encryption system uses a timestamp as part of the encryption algorithm, which changes with every packet sent?
  - Answer:
2. On its own, this is considered to be a very weak Wi-Fi protocol and easy to crack so is combined with an authentication algorithm. It is commonly used on domestic networks.
  - Answer:
3. What is the maximum data rate for 802.11n?
  - Answer:
4. Which two Wi-Fi standards use MIMO technology (you may see dual antennae on the Wi-Fi box)?
  - Answer:
5. Which Wi-Fi encryption protocol supports the Advanced Encryption Standard (AES) and is used on Enterprise networks where certificates are in use?
  - Answer:



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand and provides an excellent overview and accompaniment to this study guide.

- **Wireless Standards (5:16):** <http://www.professormesser.com/free-a-plus-training/220-901/wireless-standards-2/>
- **Wireless Encryption (3:24):** <http://www.professormesser.com/free-a-plus-training/220-901/wireless-encryption-2/>



## 901.2.6 Given a scenario, install and configure SOHO wireless/wired router and apply appropriate settings

Not strictly a router in the Enterprise network usage of the term, typical home routers are actually multi-function devices providing a number of network services. A typical router is actually the following:

- A basic firewall
- A Wi-Fi access point
- A router
- A switch
- An ADSL modem
- A DHCP server
- A DNS server

While we call them routers, they are not professional routers such as a Cisco Router, which performs routing services only.



A Sky hub (front)



A Sky hub (rear)

This section will look at some of the configuration settings you will need to familiarize yourself with, available on a home or SOHO router.



# Channels

A wireless channel is a specific range used for transmission. The channel is set on the WAP and devices will determine the best channel to use (although some end device wireless NICs allow the user to also set the channel that will be used). The range is typically 22 MHz, so is quite a narrow band. The bands are numbered and each overlap slightly. Channel center frequencies in the 2.4 GHz range start with channel 1's center frequency at 2.412 GHz, up to channel 14 at 2.484 GHz.





# Port forwarding, port triggering

The firewall usually allows only a few main ports open for common services. There are, however, 65535 x 2 ports that could be used. Some of these may allow inbound only, outbound only or two-way traffic. With port forwarding, we are adapting the IP address and port number (the socket) to a new destination, allowing the socket through the firewall and then forwarding the packet onto its destination based by information about the IP address stored in the router's routing table.

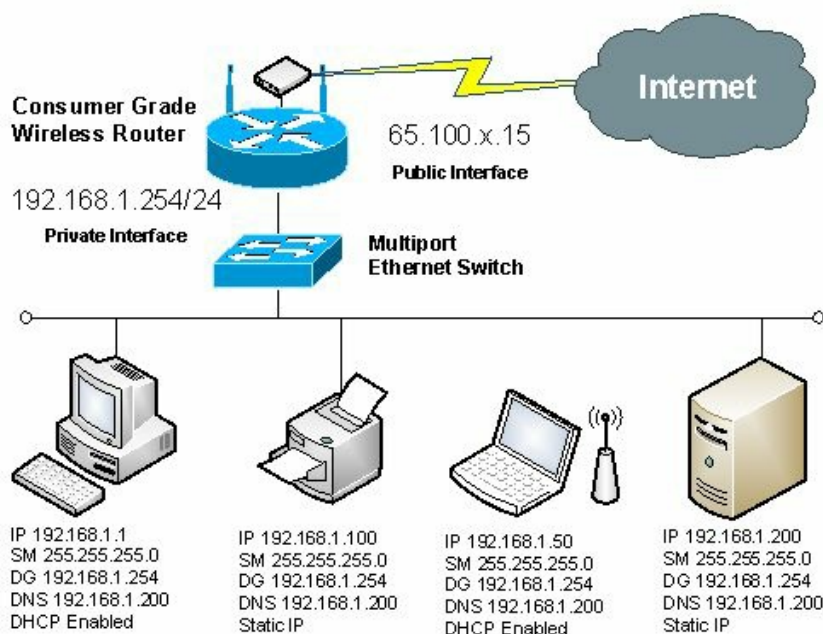
It is also possible to manage a dynamic port system where the firewall has ports closed by default. One packet sent through a common port may trigger the opening of another port (the dynamic port) allowing further data through. It is quite common with FTP to use a dynamic port. Here, port 21 establishes the connection at which point the firewall opens another dynamic port rather than the more typical port 20. When the connection is closed, the port is re-closed.



# DHCP (on/off)

The DHCP server on a domestic router is designed only to issue IP addresses and uses the class C range (192.168.0.0) with the router's IP, typically 192.168.0.1 (this is different to the Cisco router address, which is typically 192.168.0.254). The service can be switched on or off. If there is another DHCP server on the home network, or you are running a domain it is advisable to turn this off and use DHCP on the server as this has more options.

It is a common problem to see a small to medium sized company using a multifunction device such as a Sky Hub (router) to provide internet for a small network. This presents a problem in that when the company decided to run a domain, rather than a workgroup they will benefit from using DHCP on the server but may forget to turn off DHCP on the router.



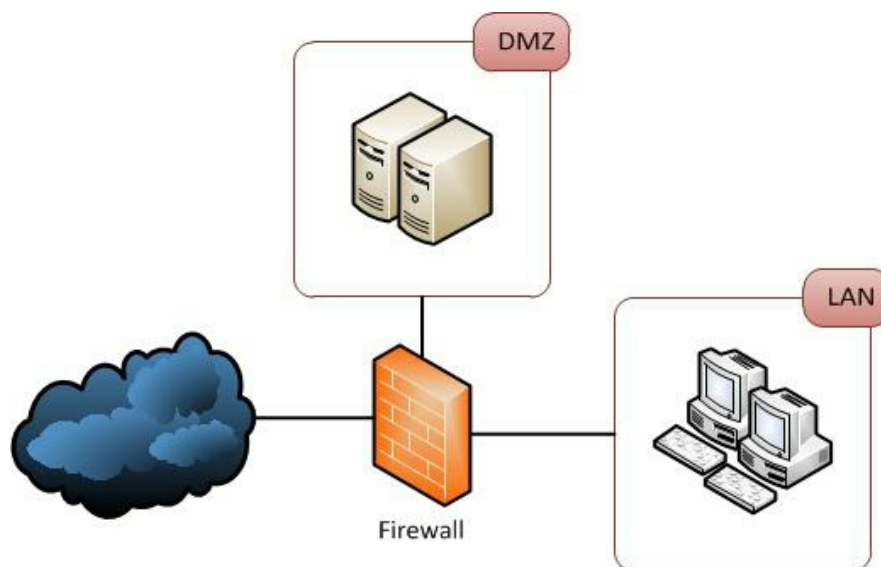
SOHO router network diagram



# DMZ

It is possible, in fact quite popular, to see a reserved, controlled area accessible from the public, but leaving the internal network protected. This Demilitarized Zone (DMZ) is a logical area housed between two firewalls in which specific public-facing services can be placed. It is possible to place the public website's web server, but also a file server should the company wish to share any documents with the public. One physical firewall may in fact create the DMZ as a third logical area - it does not have to sit in series between two firewalls.

One common trap for the unwary would be to place a logging intrusion detection software onto the file server and to leave attractive-seeming files to download. Any potential hackers may attempt to download the files and their details will be caught in the process. This is known as a honeypot, or honeytrap. A collection of such machines or dummy domain is referred to as a Honeynet.



Network security zones including a DMZ

Typical uses of a DMZ are as follows:

- File server accessible to the public
- Active Directory Federation (single sign-on)
- SharePoint server (Extranet for staff members needing to access documents when physically away from the office, or Public for members of the public to access non-sensitive documents without exposing the company network)







# NAT/DNAT

In this section we will focus on some of the router features which are significant to network design and security

- **Network Address Translation:** NAT is the process offered by a router where the packet sent from a local subnet is adapted by the router and the public IP address (or external facing IP address for internal routers) is replaced so that traffic can be sent on from the subnet to other subnets, or the wider, external network. The return packet is also checked and augmented with the internal IP address of the client PC replacing the IP address of the router. This way internal traffic can be sent out to the wider network. NAT is a vital service. Without this, each PC would need to have an IANA assigned public IP address. As it is a router can adapt internal traffic and allow it to be sent on the wider, or the external network with this feature.

**Port Address Translation (PAT)** extends the capabilities of NAT. Where NAT is the adaptation of the IP address, we can overload the IP address by also specifying the port we are going to use to communicate through. PAT is the facility for different services to travel through the same IP address (for example, HTTP and HTTPS traffic both entering the router through the router's external ports 80 and 443). This provides additional security to the monitored IP address to ensure that traffic entering from the external network is for defined services only.

- **Static NAT:** Routers can have their IP addresses assigned to their table manually, or automatically. Where the network administrator has added manual entries, we refer to this as **Static NAT (SNAT)**. This is typically used for resources on the network that do not reconfigure and the IP address is permanent.
- **Dynamic NAT:** Modern routers also communicate with each other to determine other routers, optimal paths and also some information about key IP addresses known to the neighboring router. When using NAT for the internal network, the internal IP addresses are dynamically assigned and are not accessible directly from an external source. The dynamic portion of NAT in this case refers to the fact that the routing table is self-configurable and that, as IP addresses for end client devices change, this is updated within the internal network.





# Basic QoS

**Quality of Service (QoS)** is used to bias video traffic over normal data, ensuring that bandwidth is used effectively. As well as this QoS is responsible for traffic shaping - if bandwidth reduces (for example a reduction in signal strength due to inclement weather) then QoS is able to reduce the quality of the video streamed, selecting a lower quality setting where a lower kb/s bandwidth is requested. When the bandwidth returns to a higher figure, QoS will re-shape the stream allowing a higher quality setting. This is adapted in real time.

A good example of QoS would be a news report on BBC or Sky News where the reporter is at an outside location and the video call is being beamed across to the studio via a satellite link. If the signal strength reduces, we see a drop in quality for a few seconds, but the video feed remains open. When conditions improve, QoS will use more bandwidth to increase the quality of the call.



# Firmware

Domestic routers are managed by the ISP provider (for example, Sky, BT, or Virgin Media). Periodically they will provide either a software update to the box directly using a Remote Management command and the box will update. As you are under contract, should a new version be released an engineer will fit the later version which has increased functionality.

The process of updating the router firmware (for non-managed routers for example, D-Link) requires that you download the binary file (new version of the firmware). Visit the router's webpage, log in, and there will be an upload section. After this, the router will restart using the new version of the firmware that may have increased support and additional functionality, may be more secure, and may also be more stable.



# UPnP

**Universal Plug and Play (UPnP)** is a series of communication protocols enabling a range of network devices to find each other on the network. UPnP is designed to facilitate on a home network and not across an Enterprise network.





# Exam questions

1. What is the name of the protocol used to manage and change the bandwidth of data sent across a video communication, but by doing so keeps the communication line open?
  - Answer:
2. What is the purpose of a DHCP scope?
  - Answer:
3. What is the typical lease times for wired and wireless DHCP leases?
  - Answer:
4. What reasons might you set up a DMZ/Perimeter Network?
  - Answer:
5. What is a bastion firewall?
  - Answer:



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand and provides an excellent overview and accompaniment to this study guide:

- **Configuring a SOHO Wireless Router (11:18):** <http://www.professormesser.com/free-a-plus-training/220-901/configuring-a-soho-wireless-router-2/>



## **901.2.7 Compare and contrast internet connection types, network types and their features**

Large networks may span several sites, or even countries. In order to connect where no standard Ethernet wired connection is available we will need to use a different mechanism, such as dial-up. The first part of this section will consider how we can connect by using other, non-direct means.

The second part of this section will look at the various logical network designs we can use to describe our network - its extent and size.



# Internet connection types

In a broader context we are going to focus on modulation systems used to connect networks together, forming an Interconnected-Network (internet).





# Cable

As opposed to baseband (a narrow frequency range, such as over an analog phone connection), broadband uses a wide frequency range and gives us the ability to send a large amount of data at any one time (large bandwidth).

A coaxial cable to premises connects TV and/or internet connectivity to an encoding box supplied by the ISP.



# DSL

The most common form is **Asynchronous DSL (ADSL)**, where download speed makes up approximately 80% of the download bandwidth and the remaining 20% is reserved for uploading. DSL relies on the fact that digital data transmission can be sent at higher frequencies than the human voice; therefore, within the conversion of the telephone network to digital, we are now able to send two channels of data along the same medium - lower frequency for telephone calls and the higher frequency for data transmission. With ADSL, speeds of up to 16 Mb/s are typical with advancements caused by upgrading the backbone to use fiber-optic rather than coaxial, therefore effectively increasing the possible transmission speeds and bandwidth.

Two forms of DSL are available on the market - ADSL is the most common, whereas Synchronous DSL is used by web development teams as they would have a need to upload more data than standard end users.

As mentioned previously, DSL uses a splitter box and actually leverages the existing digital phone line wiring into the premises. Each phone socket is fitted with an ADSL splitter and a portion of the frequency range is used exclusively by DSL for data transmissions.



# Dial-up

As previously mentioned, dial-up (baseband) sends an analog signal using a modem. That is a device that will generate a series of tones to represent binary data. The device also listens to incoming tones and converts them back into a data signal.

The modem uses the audible range of frequencies, so transmission is very slow. The signal at 56 Kb/s consists of carrier and synchronization data and then up to 44 Kb/s for data transfer.



# Fiber

Fiber-to-Premises is now commonplace. Here, the fiber infrastructure does not terminate at the cabinet where the media converts to coaxial cable. This gives the end user the benefit of the faster fiber speeds.





# Satellite

Again, this is a very fast transfer technology but suffers from two distinct problems:

- **Line of sight:** The satellite dish needs to be aligned towards the orbiting satellite for the strongest signal
- **Latency:** There is a slight delay in the transmission as the data stream is sent to the satellite and then bounced on to the receiving computer



# ISDN

**Integrated Services for Digital Network (ISDN)** is by today's standards a limited, costly solution but was the precursor to ADSL. ISDN lines were commonly used by business in the 1990s to provide a dedicated private line between two buildings, provided by the telecoms provider.

ISDN is a circuit-switched solution provided by telecoms providers. The line requires a dedicated ISDN modem. ISDN is in itself a data stream where the data sent is broken into discrete channels transmitting at 64 kbps. The initial ISDN model is the Basic Rate Interface (BRI), which offers 144 kb/s payload as 128 kb/s for data and then a 16 kb/s signaling channel. This is referred to therefore as 2B+D, meaning 2 bearer channels and one data channel.

The Primary Rate Interface (PRI) is carried over an E1 line and is common for corporate use. Here, we are using 30 B channels and one D channel to provide a maximum throughput of 2,048 kb/s.



# Cellular

The **Global System for Mobile Communications (GSM)** originally stood for Groupe Spécial Mobile) is a standard developed by the European Telecommunications Standards Institute to describe the protocols used for 2G cellular phone data transmission.

The original 1G system relied on circuit-switched telecommunications. It started out life as a circuit-switched system, but then extensions were added to make GSM a packet-switch oriented system. Initially, GSM was extended by the addition of the **General Packet Radio Service (GPRS)** and later with the Enhanced Data Rates for GSM Evolution (EDGE), which are still widely used as fallback systems for our 3G and 4G cell systems today.

GSM is a cellular network, so an array of aerial transmitters (cell transmitters) are needed across a city to provide coverage.

- **Code division multiple access (CDMA)** is a channel accessing method used within radio communications. Several transmitters can send information at the same time on the same channel. Each transmitter is assigned a code to maintain uniqueness within the multiplexed radio stream. This system extends the capabilities of mobile phone data transmission by allowing many different data streams to be sent from the same transmitter, on the same channel.
- **Long-Term Evolution (LTE)** is a packet-switching standard based on GSM and EDGE for use in high-data transfer and focuses on network improvements made to deliver better transmission speeds, using digital signal processing technologies. It is considered to be a global cellular standard based on GSM. It has downlink peak rates of 300 Mbit/s, uplink peak rates of 75 Mbit/s, and is considered to have low latency, therefore extremely responsive.
- **4G:** The Fourth Generation mobile telecommunications standard is now prominent as the main standard, and it can provide high-speed IP telephony, High-Definition TV, and other services where a high transfer of data is required. 4G is a cellular service and is packaged as one of two main systems: Mobile WiMAX or LTE. Current 4G transfer rates are 300 Mb/s (used when the individual is in transit) and 1 gigabit per second (Gb/s) (when the user is not in transit).
- **HSPA+:** Evolved High-Speed Packet Access is a wireless standard used on 3G networks, but it is compatible with LTE. Here, downlink speeds of 168 Mb/s and uplinks of 22 Mb/s are possible and are generated by using the MIMO (multiple

input, multiple output) wireless aerials. By using Dual-Cell HSDPA (two parallel transmission channels) and four-way MIMO, it can allow for speeds of up to 168 Mb/s downlink.

- **3G:** The Third Generation of mobile networks are the current standard for mobile communications with capable speeds typically (on its own) of 200 Kb/s.
- **Enhanced Data Rates for GSM Evolution (EDGE)** is also known as Enhanced GPRS. It is a backwards compatible standard that will operate with GSM and allows for higher bit rates per channel than GSM alone. With EDGE it is possible to determine peak rates of 1 Mb/s, a typical rate of 400 Kb/s. The extension, Evolved EDGE is a further improvement still - transmission times have also been reduced to half and bitrates have been increased to 1 Mb/s.





# Tethering

The process of connecting a laptop or PC to a cellular phone in order to access the internet via either a modem phone call or mobile data across the cellular network is referred to as tethering. The device is typically connected to the smartphone either by a Wi-Fi channel or USB cable:



Tethering via mobile



# Mobile hotspot

A hotspot is an area where the user can connect to a wireless access point (the area where the device may connect and the user authenticate to the network is considered hot). For mobile devices, it would be a specific range of that mobile device (for example, 10 meters for Bluetooth connectivity).



# Line-of-sight wireless Internet service

With the use of a parabolic disk attached to the antenna of the internet-enabled Wi-Fi access point, it is possible to direct the signal along a tight beam. This is useful to connect to a nearby building without the need for cabling. However, and especially if you are crossing public space such as a road, then UK broadcasting rules apply and you may need to have a radio broadcasting license.



# Network Types

From a conceptual and design perspective here we are going to look at the types and range of Network we can plan.

- **Local Area Network (LAN)** is a network confined within the local building or local site (a cluster of neighboring buildings defined as one site). The network is contained within one logical site. All accessing users are local to the site. A Wireless LAN (WLAN) is the extension of the LAN to support users who may be roaming but within the connectivity via a wireless router, or access point. A WLAN is more dynamic in that the user may roam across the site, connecting to different access points that serve the physical site but address themselves on the network by MAC address, not by switch port.
- **Wide Area Network (WAN)** is the extension of the LAN in that it is a variety of network resources (usually a department, PCs, or specific users) who need to work away from the main office location. The connection of a branch via a secure Virtual Private Network (either a dedicated leased line or a secure IPSEC tunnel through the Internet network) will extend the capability of the network to other users based away from the head office. The remote user will have exactly the same experience as if they were logging on at the head office.
- WANs come in various types but is a general rule the term WAN refers to any remoting user attaching to a main network located within one central building (the LAN).
- **Personal Area Network (PAN)** is a small, discrete network, usually ad hoc in nature, that enables the user to create a connection with neighboring devices in order to transmit data. A PAN is typically Bluetooth or Wi-Fi and would be a direct link between two devices. For example, a smartphone can connect via Near Field Communication (NFC) to transmit a file to a wireless printer in order to print a copy of a document. Also, two smartphones may connect via Bluetooth and send an image.
- **Metropolitan Area Network (MAN)** - Where there are two or three defined areas within one city, we refer to this as a MAN. Usually, the MAN sites are connected by a leased line or secure tunnel making use of the existing internet infrastructure within a city. WiMAX and Metro Ethernet are ideal systems to support the creation of a MAN and negates the costly need of a leased line to send trunk data between sites.







# Exam questions

1. I am located in a university building. This has a connection between several buildings making up the campus, located within the city I am in. The university has three campuses across the city - all are connected together. I have a video conversation and share a file with my friend who is located at one of the other campus buildings. What network is used here?
  1. MAN
  2. CAN
  3. PAN
  4. LAN
2. I want to share a photo by Bluetooth with my friend sitting opposite me. We both are using smartphones with Wi-Fi, infra-red, and Bluetooth enabled. What network is used here?
  1. MAN
  2. CAN
  3. PAN
  4. LAN
3. I share a file across the domain. My PC is wired to the wall outlet at my desk. The recipient is on the same floor in a different room, in the same building. Her PC is also connected via a wired Ethernet cable. What network is used here?
  1. MAN
  2. CAN
  3. PAN
  4. LAN
4. What is the current transfer rate for 4G?
  - Answer:
5. For the Internet Service Provider, what is the benefit of Fiber-to-Cabinet over Fiber-to-Premises?
  - Answer:



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand and provides an excellent overview and accompaniment to this study guide:

- **Internet Connection Types (7:36):** <http://www.professormesser.com/free-a-plus-training/220-901/internet-connection-types-2/>
- **Network Types (3:21):** <http://www.professormesser.com/free-a-plus-training/220-901/network-types-3/>



## **901.2.8 Compare and contrast network architecture devices, their functions, and their features**

I wanted to discuss this much earlier in the chapter, but have deliberately held back until now. This section is going to look at the actual physical components - the devices you will connect through and to, which make up your network.



# Hub

Simply put, hubs are stupid. A hub is a simple electronic device that replicates the electrical signal sent on one port and sends this signal out on every other port. The receiving devices have to check the header information on the frame to determine if the data frame is meant for them. If not, the data frame is discarded, but this clearly stops the NIC from being able to send out data frames of its own at the same time as the line is busy. Hubs are therefore only used when connecting a small network, such as a **Small Office Home Office (SOHO)** network or might be used for a connection point on a network where there is no concern over when devices might access. For example, if we have two PCs wired into the network and a hub provides the interlink, with only one user and only one PC likely to be used at any one time, then there will be no congestion and the use of a hub can be justified.

The important takeaway is that, unlike a switch, a hub does not store any information concerning ports and therefore is not aware of the rest of the network other than the completion of an electrical circuit through the connection of a network cable to a live device. There is no on-board computer storing a MAC or IP table and so no means to manage the flow of data. Hubs are, however, very inexpensive and are a simple solution. They should never be used as part of a more complex network, or as a central connecting device:



An OSI layer 1 hub







# Switch

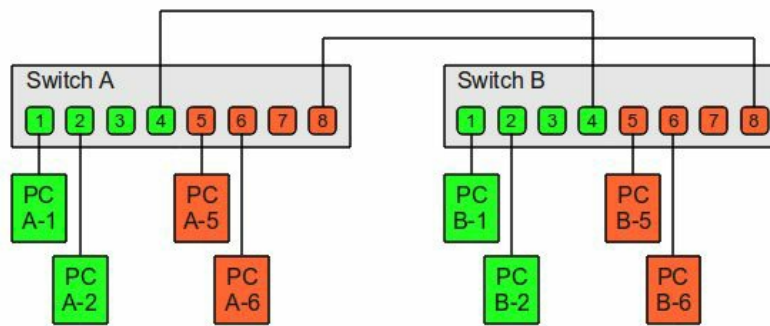
As opposed to a hub, a switch is a device that allows data to be sent within the local subnet. It is a physical device acting as a central wiring point where each local PC is connected to the rest of the network. Where a hub would copy the electrical signal and replay this on every other port, a switch is able to determine which port the data is required and a virtual connection is created between the two ports allowing other virtual connections through other unused ports. A switch is therefore extremely efficient as there may be many different data streams being sent through the switch at the same time. The switch is able to deal with each data request without loss of data or data collision.

A switch is a device operating at layer 2 of the OSI model. There are typically two types of switch that we will encounter here:

- **Unmanaged switch:** This is a dedicated device capable of transferring data from one port to another with a very fast turnaround time. The switch keeps a basic table of port and MAC address of the NIC connected to that port and this table is updated regularly. Once the MAC address is learned, the switch can use this data to determine which port I need to send the data on to. This form of switch does not operate at layer 3 OSI - it cannot work with IP addresses and does not have a management web page. It cannot accept ICMP requests (for example, you cannot PING an unmanaged switch).
- **Managed switch:** A managed switch, also called a multi-layered switch because it has a web-based management portal to configure the device can provide additional functionality. One common control would be to set the direction of traffic as one-way or two-way, also if it is one way which actual direction the data should be sent (uplink or downlink), also to set the speed (baud rate) of the connection on a specific port. As the device has an IP address in order for the administrator to effect changes to the device, the device is said to operate at both layers 2 and 3 of the OSI model.

One common advantage of using a switch is the fact that, as with routers, a switch can communicate with another switch to determine the best route through the network. While it is common to see switches within one building, it is only usual to see a router be used to connect the subnet to another subnet, or to another part of the network, or even to the internet. These switches are configured using a management web page. They can accept ICMP requests from other devices on the network and you can set up logical groupings

by connecting ports together to form a Virtual LAN (VLAN). Managed switches can also operate as a cluster of switches, and VLAN ports can extend across all of the switches in the cluster.



A VLAN across a switch cluster



# Router

A router is a device designed to act as a doorway allowing data traffic out of the local subnet. Devices are connected together logically by using a numeric grouping system called IP addressing. Each device is informed of another IP address within the same internal subnet that is the gateway point through which it can direct traffic onto the larger network.

As with a physical door, it has two handles (or IP addresses), one on each side (the internal network and the external network).

Routers operate at layer 3 of the OSI model, and by so doing, they manage access to other networks by using the IP address and subnet mask of each data packet being sent. The IP address is split into two portions - the network portion and the host portion - and so the subnet the data is being sent on to is determined.

Routers are relatively chatty themselves. Routers have their own common language (the Routing Protocols), and several of these are covered later on in this course. As with switches, a router contains a small computer that stores a table containing the IP address of the connecting computer and the physical port it is connected through. Unlike a switch, which stores the physical MAC address of the NIC, IP addresses are used and one cable may carry traffic from an entire group of computers (the subnet).

Routers use their own routing protocols to talk with other routers to determine which other subnets are serviced, and by so doing can determine the best route to get to a particular part of the network. Different routing protocols work in different ways, but it is interesting to note that this is an automatic process and allows a router to be aware of other connections beyond its own physical confines.

Routers are also designed to block traffic not intended for a specific device. Broadcasts, namely a packet intended for everyone on the network to hear, would cause congestion on the wider network, and so the Request for Comments paper RFC 1542 details the need for routers to effectively block broadcasts. Without this the internet or the local network would become congested as PCs try to discover network services. This is particularly true for two network functions:

- **Imaging and deployment:** As part of the imaging process, the image and the preliminary pre-installation environment are streamed across the network to the

waiting PC, which initially has no data on the hard drive. The PC boots up from data received across the NIC. The protocol that is involved in this process is the BOOTP protocol, so if a router is in the way of the data stream it will effectively block the process and stop the image data from reaching the waiting PC.

- **DHCP:** The DHCP service allows client PCs to request and obtain a leased IP address for a length of time. Part of the process involves the sending of broadcast packets. If a router was in the way of the data flow, the server may not be contacted and the DHCP process may not even begin.

Routers are also capable of adapting traffic so that a device designed for another network can be adapted and the reply data can also be adapted. The process, referred to as Network Address Translation, enables the router to remember the IP address of a sending PC on its routing table, and it is very common to see this process in use on the external-facing router as this service negates the need to put individual public IP addresses for each PC in the organization. Instead, we can use one public IP and share this amongst every PC on the network. It works as follows:

- The PC wishing to send data to the internet (the public network)'s IP address is recorded on the router.
- The router removes the sending PC's IP address from the return data and replaces it with its own IP address.
- The augmented packet is sent across the public Internet.
- The returning data is addressed to the router's external IP address, but the router realizes that the packet needs to be sent on, so the incoming packet is augmented and the external IP is replaced by the original PC's IP address.
- The augmented packet is sent across the internal network

Finally, it is important to remember that we are concerned with data security starting by protecting our own internal data. The router is a bastion of protection for our local network, so it is helpful to think that the router is a line of defense rather than a means to connect beyond the network. We therefore talk about blocking data coming into the network rather than extending capabilities of the internal network.





# Access point

This is a device that allows connecting devices to access the main network. This is typically a wireless access point - a device that can re-transmit wireless data as wired packets across the wired network. Loosely speaking, an access point on an ad hoc network is another laptop's wireless NIC.

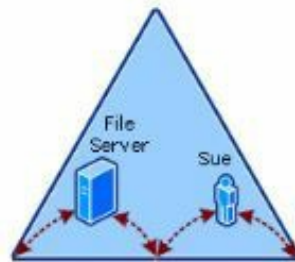


A Wireless Access Point



# Bridge

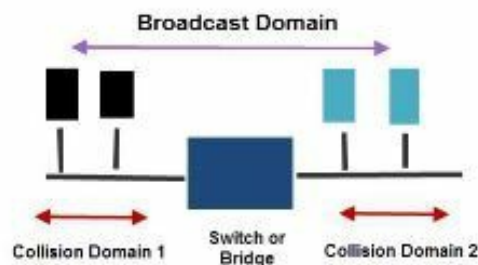
A bridge is a device that can be used to physically connect two separate sections of the network together. These two separate sections may be logically different; the data from subnet A may have to pass through subnet B to get to the wider network, or out to the Internet. The physical extent data can be sent is referred to as the Collision Domain. In the example here, without a bridge to connect areas A and B together, data sent within A stays within A and cannot reach B.



A collision domain

A bridge does not act upon the data being sent - it does not partition the data in the way that a VLAN will do using the VLAN ID, or a router will do using the IP address.

What we are describing with these logical groupings is a Broadcast Domain (BD), which is different to a Collision Domain. A BD is logically defined. It is the area that defines the boundaries of the domain itself. It is usually the collection of PCs and switches that make up the subnet. The domain is usually ended at a router because routers are set to block broadcast packets. A broadcast domain might consist of several PCs in several buildings spanning different countries and is not defined by physical location:



A broadcast domain





# Modem

An analog modem performs two roles - to convert from a digital electronic signal (as with a NIC) to an audible generated tone which represents an analog number. This tone can be transmitted along the traditional voice phone network (as engineers in the United States would refer to it, the **Plain Old Telephone System (POTS)**). The term modem refers to the two roles: modulator (to generate a noise) and demodulator (to read the audio signal and recode it as digital binary data). A modem would typically connect to a PCI or ISA (or CMR) slot on the mainboard and would connect to the phone line. A telephone can also be added to the modem in order to make standard telephone calls when the modem is not in use. More advanced modems also support the sending of a fax, which is why it became a popular tool for early networking.

Analog modem speeds were very slow by today's standards at approximately 56 kb per second, so a typical web page with only three small GIF images and approximately 200 words of text might take up to 8 - 30 seconds to load. A modem is therefore not an effective tool for today's networking.



A dial-up modem



# Firewall

This term tends to mean different things to different people. While it is true that there is a software firewall (in fact, with Microsoft systems there are two firewall screens available to you) built into the PC, there is a hardware firewall - an expensive but dedicated device designed to limit data from accessing your network. Each data stream is allocated a number that determines the type of data being sent through the network. These are controlled by two different transport protocols:

- **Transport Communication Protocol:** TCP is used to ensure that data sent is received correctly and is said therefore to be a reliable protocol. With TCP, the two PCs will first attempt to handshake, that is, to establish communication before any data is sent. If a packet receipt is not received in good time, then the packet is resent. Therefore the receiving PC can maintain and check the packets as they are received until the file is re-structured. There is also a degree of error-checking taking place which ensures the validity of the data received. TCP is therefore a very reliable protocol, making it good for file transfers.
- **User Datagram Protocol:** UDP is not a connection-oriented protocol. Here, a stream of data is sent. There may be errors in the data stream and there is no consideration as to if the data is being received or not. As there is no error-checking mechanism built into the packet, the packet can contain slightly more data, making receipt a little faster, but the data stream will be prone to errors. This, however, makes it a good protocol to use for video conferencing, online video streaming, and webcam streams where the end user will not be too concerned if there is a slight glitch, or where the user may want to opt in or out of a video conference.

There are 1,024 system ports (from 0 to 1023), which are known as the commonly known ports. Above this, 1024 to 49151 are the registered ports. They are registered with IANA.

As well as port numbers, a software firewall can trigger the opening of a port based on an application requesting it. This will be on a temporary basis, and when the job is done the port is re-closed. Dynamics ports are opened through application rules, and this service would usually feature on either a software firewall with advanced security or on a host-based intrusion detection system/internet management software.





A high-end hardware firewall



# Patch panel

A patch panel is an endpoint for a connecting cable taking data from a room socket. It is labeled with the same ID number as is on the socket and from the panel. Further patch cables can take the data to a specific port in a local switch. By doing so we can then provide data management and transfer to the correct port and then to its destination. For our purposes, the patch panel is an interface device allowing us to extend from the switch to the NIC. A patch panel contains no intelligent circuitry; it rather extends the run of the line from the switch to the NIC.



An IDF patch panel



# Repeaters/extenders

A repeater is a device designed to regenerate the incoming signal to then send it further. Repeaters are placed at the end of a run of network cable in order to extend the distance further. A common example is the Fiber Coupler- this is a junction box-style device capable of extending the run of a cable. They are typically used in underwater repair where the cables have to be joined together, but are essentially dark boxes where the two fiber cable ends can be joined and the signal repeated. Advanced couplers can read and re-transmit the data stream, acting as a repeater to extend the length (the run) of a data stream over several miles.



# Ethernet over power

The earth wiring within the ring main of a domestic home is not commonly used by devices other than to earth the device, meaning that its voltage is the same as that of the Earth (not 0V, though). All devices share the same earth voltage, as do anyone who touches the bare metal exterior of the equipment.

With this in mind, what if we were to send a low-power signal across the ring main? Effectively, we can leverage the fact that we already have a cable laid within the home and therefore can use power sockets as if they were network access points.

It would, however, be incorrect to assume that the earth wire is solely used. Power is transmitted at 50 Hz (in the UK) and in order not to interfere with this, Ethernet over Power (EoP) sends data signals at 3 kHz.

In the UK, using EoP devices in a built-up area where it could affect other people, such as in an apartment, have led to legal challenges under the concern: undue interference with wireless telegraphy apparatus. This is therefore not an ideal solution and at the moment is targeted for use by the domestic market where there is no chance that your actions could interfere with your neighbors.





# Power over Ethernet injector

This is commonly used as a strategy to power devices such as webcams or CCTV cameras directly from the switch negating the need for external power supplies. This is extremely helpful in situations where cabling to devices needs to be tamper-proof or hidden from the elements (as CCTV cameras are used often externally).

Other devices that make use of PoE are PTZ cameras (motorized cameras with pan, tilt, and zoom motors built onto the camera). The camera is mounted onto a gyroscope gimbal and can be remotely controlled. These are often used within TV studios (for example, in the reality TV show Big Brother). IP phones and remote Ethernet switches can also be PoE powered.



PTZ camera

The cable can be used to provide both data and power to the end device. PoE allows us to transmit power over long distances, making this a good solution for CCTV and a better solution than USB, which has a limited range.

Twisted pair cabling uses differentiated signaling, which has the effect that power will not cause interference with the data being transmitted.

The switch would act as the PSE, and the end device to be powered is referred to as the powered device. The powered device is able to request its power requirements, and power can be increased as needed. With PoE (IEEE 802.3af-2003), 15.4 W (with an assured 12.94 W) is available for the device.

**Power over Ethernet+** (IEEE 802.3at-2009) is an update to the PoE standard. It

allows for up to 25.5 W, although all four pairs within the Ethernet cable cannot be used to supply power. A theoretical 51 W can be transmitted.

I was once visiting a military base and was advised not to plug my laptop directly into the network. Their switch ran PoE, and if my MAC address was not on the MAC allow list then a pulse would be sent to my network card, damaging it....Suffice to say, I did not test it.



# Exam questions

1. Which network device separates logical areas of the network?
  - Answer:
2. Which network device separates physical areas of the network?
  - Answer:
3. Which network device joins physical areas of the network passing logical information into the wider subnet?
  - Answer:
4. Which network device restricts data packets by the purpose of the data?
  - Answer:
5. Which network device duplicates the signal to all other ports it can send to, but restricts other devices connected to it from being able to send at that point in time?
  - Answer:



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand and provides an excellent overview and accompaniment to this study guide:

- **Network Devices (9:43):** <http://www.professormesser.com/free-a-plus-training/220-901/network-devices-2/>



## **901.2.9 Given a scenario, use appropriate networking tools**

In a previous section, we looked at a range of networking tools and how they worked, but how do we remember which ones to use in different scenarios? What follows are some sample scenarios you might like to refer to, to consider when each tool is used.





# Crimper

This is used to cut a network cable (it has a cutting blade) as well as to secure the RJ-45 or RJ-11 connector to the cable end. The metal pins are squeezed down onto the cable wires, piercing the sheath and holding the wire in place, while making connectivity with the copper wire below. Secondly, the plastic lock is pressed down and onto the outer PVC of the cable, holding the connector tight to the cable.

If a cable is damaged, the crimper can be used to cut the wires to the correct length and enable you to fit a new connector.



# Cable stripper

This is similar to the crimper and the terms can be used interchangeably, but one form of cable stripper is a circular doughnut-style blade designed only to remove the outer sheath and is not used to fit the connector:



A cable stripper



# Multimeter

The multimeter is used to check for voltage and to get an accurate reading. It has three modes and can measure voltage, current, and resistance.

To measure the voltage on a circuit, check that the dial is set to read the correct scale (otherwise you may damage the meter) and hold the probes across the component you want to check (for example, either side of a resistor). To measure the current, the meter is placed in sequence before the component you want to check. To measure resistance, hold the probes at either side of the component you want to check.

For example, to check that a Molex plug is issuing 12V I would place the black probe on the pin connected to the black wire and the red (live) probe on the pin connected to the yellow wire. You will get a reading that will slightly fluctuate but not go over 12V.

If when measuring resistance you get a reading of infinity ohms, this would indicate an open in the circuit (referred to as an open circuit, or a short), for example, a blown fuse. Also, if you hold the two probes to each other you should get 0 ohms (closed circuit).



# Tone generator and probe

These are often referred to by the main manufacturer Triplet's Fox and Hound. Imagine an IDF with hundreds of Ethernet cables and you need to identify the other end of a specific cable. The known end of the cable is fitted to one of two devices that make up the Fox and Hound. This powers the cable and sends a signal that can be picked up by the probe, at which point it will emit an audible sound. In the IDF, you would then touch the probe against each Ethernet cable connected to the patch panel until the correct cable is located:



Fox and Hound toner probe



Some high-end offices rent their building space and the building owners are responsible for the upkeep of the building's network infrastructure. It is common to see a fiber strand within the jacket of the Ethernet, or fiber-optic cable which, once a button is pressed on the switch in the IDF, the other end of the cable will illuminate. However, these are not commonplace.





# Cable tester

So, you've just laid and made up an Ethernet cable and crimped the connectors onto either end. Before the cable can go into use, we need to test that all of the wires have good connectivity.

The cable tester sends a pulse of electricity along each wire in turn to illustrate that the RJ-45 connector is making good connectivity with the cable wires:



A cable tester

One variant of the basic cable tester is the cable certifier. This is not covered at A+ level but it would be useful to know that this also exists. The certifier is used when laying cable within the building infrastructure and confirms that the cable conforms to building and electrical regulations. It not only checks for a voltage on the cable but also the level of signal, ensuring good connectivity along the cable:



A cable certifier





# Loopback plug

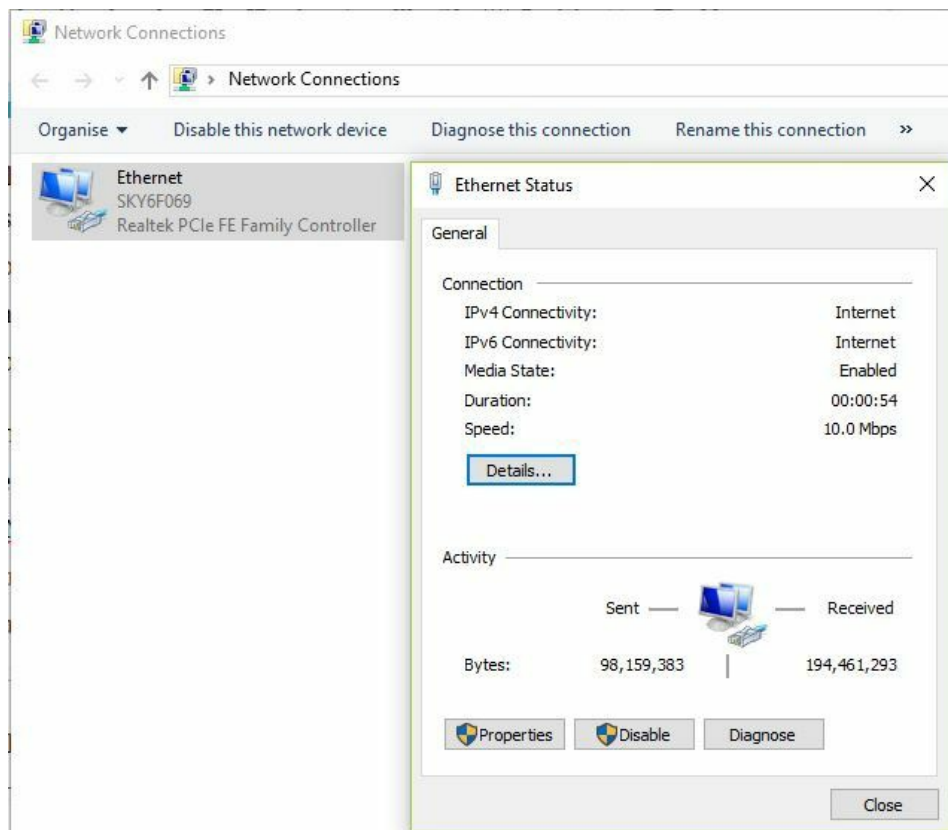
For the matter of a few pence you can make this important, invaluable tool. Simply use two Ethernet wires (only a few inches of wire is needed) and connect pins 1 to 3 and 2 to 6 in an RJ-45 connector. Plug this into the NIC you need to check (with the PC powered on) and you will trick the operating system into thinking that a network cable is connected as it can see handshake data being sent and received on the respective pins.

Why do this? Imagine there may have been damage to the unit. For example, a laptop was dropped onto the floor and landed on the NIC, or an end user got their foot caught against the network cable and pulled it out of the NIC. This may have damaged or dislodged the connecting pins in the port itself. If you decide to run a PING test on the command line, you will get a result because the TCP/IP protocol stack is being used by the operating system - as far as it is concerned everything is fine, but a PING test does not check the condition of the physical network port.

This makes for a good check for an end user system not connected to a network via a switch. If the device is connected to the network via a switch, a successful PING test to another device on the subnet will also prove that you are able to send and receive data through the port, therefore the port must be OK.



NIC with no cable connected



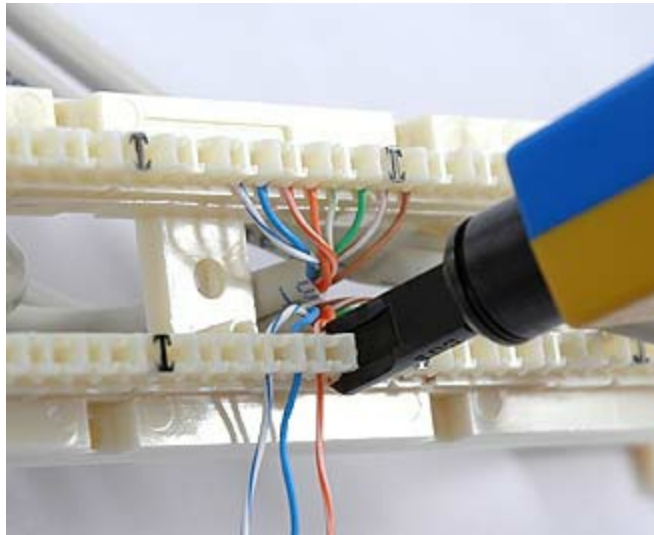
Network Connections and status form now showing connectivity



# Punchdown tool

If you are fitting a network wall socket, or adding a cable to a patch panel (110 block) in the IDF, you will need a punchdown tool. Both of these connections use a series of metal blades in a V-shape and a slit at the base. The wire is caught within the slit and as it is lowered into the slit the plastic sheath protecting the wire is cut into. Connectivity is through the V-slit direct to the metal wire.

This does require some force, so a spring-loaded punchdown tool is used. This locks on top of the V-slit and is used to push the wire down and into the slit, piercing the protective plastic as it is lowered.



110 block and punchdown tool

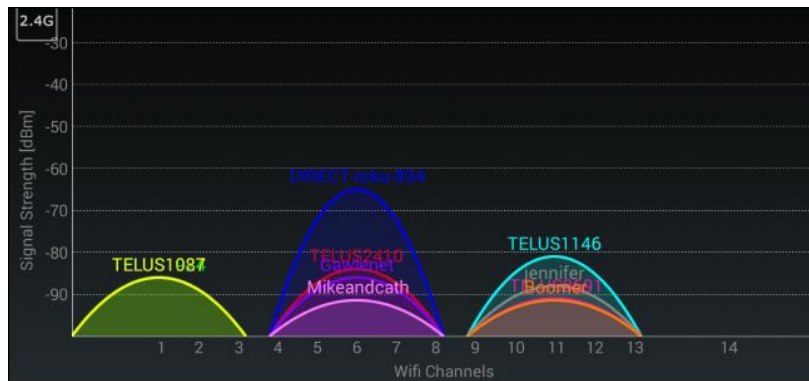




# Wi-Fi analyzer

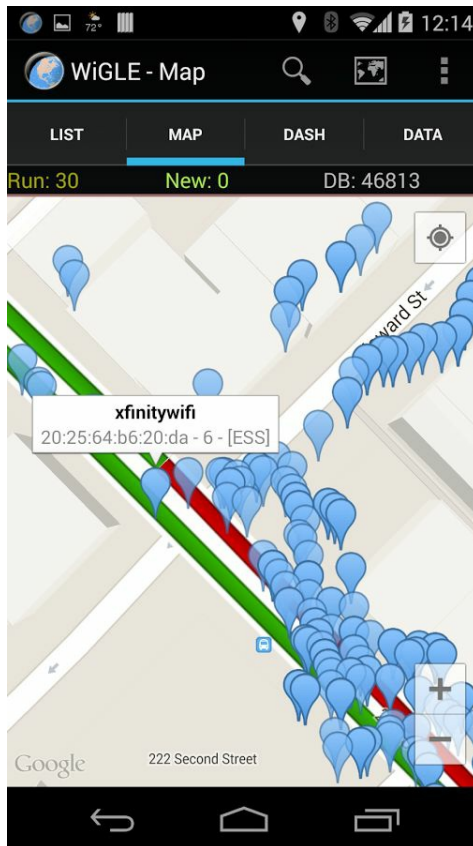
While you can buy this as a proprietary tool, it is common to use a simple smartphone with a Wi-Fi analyzer app installed. It will show the different Wi-Fi networks within range and report on the signal strength of each, and which channels are in use.

This is used to physically scan a network, checking the signal strength of wireless access points within the building.



Wi-fi Analyzer

An alternative analyzer can be used in war-driving (that is, the process of driving around a neighborhood and recording onto a geographical map the different networks found listing whether they are open or closed (also listing their authentication and encryption), as a heat map.



A war driving heat map



# Exam questions

1. Which device is used to connect an RJ-45 connector to an Ethernet cable?
  - Answer:
2. Which device is used to check a local area for Wi-Fi hotspots and show the encryption, SSID, and authentication protocols used?
  - Answer:
3. On which hardware is a punchdown tool used?
  - Answer:
4. What three things can a multimeter test for?
  - Answer:
5. Where would a toner probe be used?
  - Answer:



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand and provides an excellent overview and accompaniment to this study guide:

- **Networking Tools (7:13):** <http://www.professormesser.com/free-a-plus-training/220-901/networking-tools/>





# Summary

To a person just starting out, networking is both a challenge and a reward. It allows you to flex your IT muscles on devices and concepts beyond that of the end user device.

While you may be limited in your role as to how much access you will get to the rest of the network, rest assured that sooner or later the problem will not be with your end user's device, but elsewhere on the network. Where a service is affected, several or in fact all of the PCs within an area serviced by that server or device will not be able to use the service. The problems are much larger and the fixes more complex, but as I say, rewarding.

These first two chapters are absolutely vital to your understanding of the A+ certification. Together they form 55% of the material and if you have understood the networking section, that will help you later on as the next exam typically taken after A+, the CompTIA Network+, covers just the same material as you have covered here in this section, and extends on your knowledge of this fascinating area.

The next chapter is going to shift our focus onto completely disconnected and portable devices - mobile devices, starting with the laptop, but also considering variants, and variants of the smartphone, leading through the recent growth in personal wearable tech.



# Mobile Devices (901.3)

We will start this chapter by considering how we can attach storage and additional functionality to mobile devices unique to laptops. We will then look specifically at the internal hardware specific to the laptop. We will look at features specific to a laptop and consider scenarios when they might be used. We will then compare and contrast different other mobile devices, and then look at ports and external connectivity to these other mobile devices.



# **901.3.1 Installing and configuring laptop hardware and components**

In this section, we are going to specifically look at laptop hardware. Laptops are minified hardware systems often with bespoke circuitry designed to fit into the case, whereas PC systems follow standard form factors.

The laptop is defined in terms of size by its screen dimension (diagonally, corner-to-corner) that defines its size as a laptop. The thickness and weight of the laptop are also key factors.

The ultimate aim of this chapter is to realize that most laptop parts are specific to the make of the laptop and with the exception of expansion cards or RAM modules are quite bespoke and intended to fit into the case that is molded around these parts.



# Expansion options

Common hardware with all laptops are the expansion slots allowing for additional functionality not covered by the base motherboard. As laptop sizes reduce so to do the opportunities for expansion and also the number of ports you can have to connect peripherals. This can be overcome with only one port (for example, a USB hub is ideal for connecting a variety of devices), but functionality is shared meaning that data bandwidth is not at its most optimal.

What follows is a variety of expansion cards that have existed for laptops over the past 20 years. We are going to look at the different ways in which we can add additional functionality to the main device.



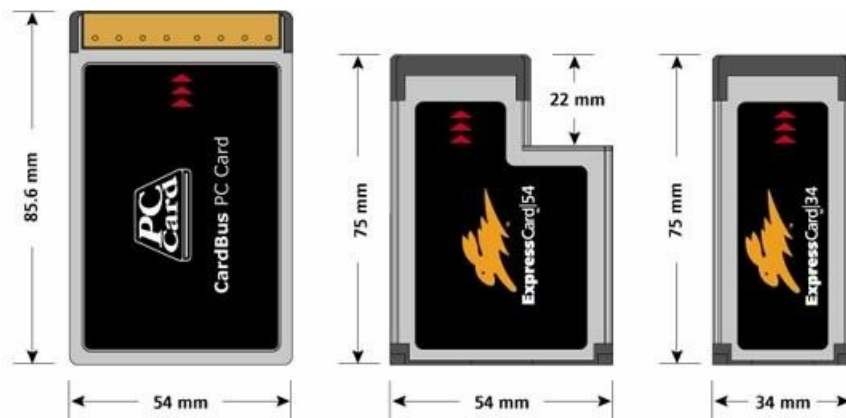


# ExpressCard /34

As a PC has PCI slots for new cards to be added for additional functionality, a 'common purpose' slot has been added to the laptop, known as the ExpressCard. The slot is generic and you can simply install and remove the 'card' of your choice, adding additional functionality to the laptop.

ExpressCards allowed for a variety of different additional functions, but were commonly used to communicate with other data ports not otherwise available. For example, early laptops, or laptops designed specifically for docking stations, did not have NIC capability, so this was provided through the ExpressCard.

The ExpressCard is measured by the width of the slot in which the card was placed. The two widths in use are 34 mm and 54 mm.





# ExpressCard /54

The 54 mm is backwards compatible - it can support the 34 mm cards.

The ExpressCard slot connects to a series of different busses on the motherboard. The ExpressCard device you are inserting will interface with one of these busses, but the bus will differ depending on the functionality of the ExpressCard being inserted.

The ExpressCard speeds you will encounter are:

- 480Mb/s (USB 2 mode)
- 5Gb/s (USB 3 mode)
- 5 Gb/s (PCI Express bus mode)



# SODIMM

In previous chapters, we looked at some of the full-size RAM sticks available

The laptop equivalents had a smaller form factor. SODIMM is in fact approximately 2/3<sup>rd</sup>s the size of its PC equivalent. Typically, there are two RAM slots in a laptop, either side of the motherboard. One is located on the rear and is accessed by removing a back plate; the other requires you to remove the keyboard to access the slot.

## DDR standards and pins:

DDR SDRAM Standard	Release Year	Bus Clock (MHz)	Transfer Rate (MT/s)	DIMM pins	SO-DIMM pins	MicroDIMM pins
DDR1	2000	100-200	200-400	184	200	172
DDR2	2003	200-533.33	400-1066.67	240	200	214
DDR3	2007	400-1066.67	800-2133.33	240	204	214
DDR4	2014	1066.67-2133.33	2133.33-4266.67	288	256	-



# Flash

Flash memory refers to an EEPROM stick. This is non-volatile, meaning that if the power is switched off then data is retained. This is used as a storage device. Due to its small size and relative low cost at approx £1 per GB this makes for a cheap and simple way of moving data from one PC to another. Data is now mobile.

But then hasn't it always been? Yes. It's only a matter of perspective. In the 1980s we used 5 1/4 inch floppy disks. In the mid to late 1980s these became 3 1/2 inch floppy disks (small enough to fit into your coat pocket). As a school student I remember that my blazer always contained my **Book of Psalms** for morning assembly, my homework diary, a few pens, a calculator, and at least one floppy disk.

Back then (1990) one floppy disk could hold 1.4 mb. At a computer trade show in 1981, Bill Gates supposedly uttered this statement, in support of the new IBM PC's 640KB usable RAM limit: 640 K ought to be enough for anybody.



Digital Equipment Corp. founder Ken Olsen also famously stated: There is no reason for any individual to have a computer in his home. Here, he was referring to home automation, not PCs in the home, but it is encouraging to see how IT has moved on - we now have PCs, laptops, smartphones, tablets, phablets, and home automation!

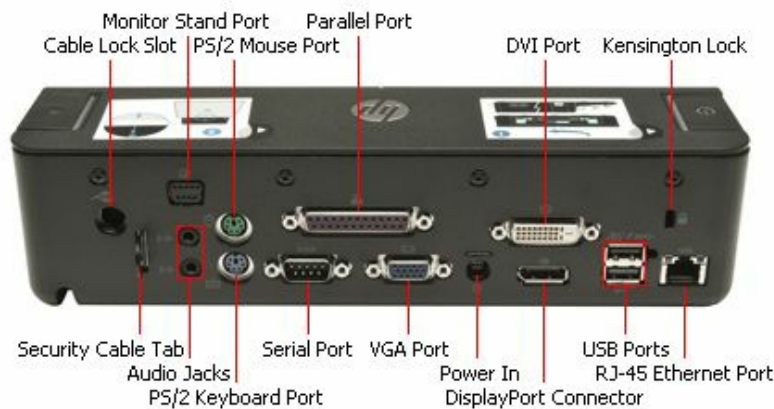




# Ports/adapters

The laptop used the same ports as you would find on the PC, making them interchangeable as an office and home solution. However, docking laptops were missing a variety of ports that were common place on the PC. By using a docking station we allow the user to take the main device away and work on files away from their desk, then come back to the desk later on to upload the file to the network.

HP laptops were extremely thin and small. These lacked the capability of adding devices directly to it and so a docking station was needed. A common SCSI-type port on the base of the laptop was used to connect and lock the laptop into place against its station.





# Thunderbolt

As in 901.1.4, developed by Apple and Intel, the Thunderbolt is commonly found on Mac systems such as the MacBook Air. It was first launched in 2011 and uses a Mini DisplayPort connection (more on that later). Modern equivalents now use a USB type C port.

Thunderbolt can transmit PCI Express and DisplayPort data as well as providing DC power, which makes them ideal to attach to recording devices such as digital movie cameras. Thunderbolt C can transmit at 40 Gbit/s (5 GB/s), surpassing FireWire.

The idea here was for ultra fast data transmission of high-quality media data, and that was where it was marketed.

Also note that the Thunderbolt interface was also a Mini DisplayPort interface. These are in fact the same connector.



# DisplayPort

The DisplayPort was specifically designed to carry image and data, whereas the Thunderbolt was designed for high-speed file data transfer. However, in reality as the Thunderbolt could also do the job of the DisplayPort the Thunderbolt was the better choice as it allowed for media transmission and also very high speed file transfer.





# USB to RJ-45 dongle

If it were not for the requirements needed from laptops USB might not have become the dominant standard. For years it contested with Apple's FireWire to a point where eventually USB won out and Apple now supports USB.

**USB** was just that--a **Universal Serial Bus**. A bus that could change its speed depending on circumstance and not the other way around, as is the case with ExpressCard.

USB to RJ-45 clearly did exactly what it says. We get 100MB/s or 1GB/s network transfer speed across an ethernet cable. This dongle was designed for laptops that might have one USB port, but no Ethernet network capability.







# USB to Wi-Fi dongle

Equally USB as the common port can also provide Wi-Fi access. They are also quite discreet.





# USB to Bluetooth

As with the previous dongle, Bluetooth was not native to most work laptops. To provide the access to a PAN network we can share to local devices using a simple Bluetooth connection that requires only a common PIN code set on both devices.





# USB optical drive

Modern PCs no longer have space in the chassis for a CD-ROM drive. A number of lightweight laptops also are too thin to hold an optical drive. Given the fact that the propensity of USB has meant that most superficial data transfer takes place via USB, optical might seem redundant, however, it does still have its place.

Optical DVD / CD-ROM discs are commonly used as installation discs, also for audio, or to play movies. This has not changed since its birth to the UK in 1982.

To assist with this USB drives can also support mobile optical drives. These are often used by technicians to install an operating system, and then remove the hardware shopping would-be hackers from trying to circumvent the existing system.

Remember that the BIOS / UEFI needs to support USB booting in order to use this for PC/laptop booting, overriding the existing OS bootstrap.





# Hardware/device replacement

Whilst it is good that the mobile device is small, compact, and lightweight it does have a number of flaws from a maintenance perspective, so it is necessary to add additional functionality that otherwise would already have been there with a PC.





# Keyboard

The most obvious is the keyboard. The laptop keyboard is condensed with many keys performing additional functions, but it is also notable that a number of devices, for example, Phablets or small laptops with one USB port have no hardware keyboard at all. Here, if there is a problem with the OS it is not possible to hit the escape keys (the built-in key sequences known to the IT technician to get access to the backend menus) and from here on run the system in maintenance-mode (referred to in the Microsoft world as safe mode).

A modern PC keyboard contains 104 generic keys. The more pertinent point is how these keys are accessed - if your keyboard is OS driven (for example, a wireless keyboard connecting through a USB dongle) then the keyboard is not present and able to be used until the software and driver responsible for the USB interface is present. This interface is governed by the OS, so the OS needs to be loaded first.

I recently went to help out a friend who had a corrupted hard drive. The OS (Windows 10) would not load. Their keyboard was a USB wireless keyboard. I explained that the keyboard would not work until the OS was loaded and as they had no OS to load, the only alternative was a direct connection so that I could manipulate the BIOS.

Traditionally this would be through a PS/2 port, but modern motherboards also support USB natively.

I brought along my keyboard, borrowed their Windows installation disk and managed to trigger safe mode. However, the system was irreparable, so the hard disk was wiped and the OS reinstalled.



# Hard drive

An external hard drive usually connects through either an e-SATA connection (an external port otherwise connecting to the SATA bus), or via USB or similar port. The hard drive on a laptop is 2/3 the form factor of a standard PC. Power consumption is lower and on modern laptops is SSD in nature, which gives both benefits and disadvantages, which we will look at in further detail in the following section.



# SSD versus hybrid versus magnetic disk

The magnetic disk is vulnerable to physical shock. It has slower access speeds than SSD, but is considered a more reliable medium. Magnetic disk is still used for the majority of corporate archiving.

A hybrid disk is a combination of both - the slower but more reliable drive is used in one partition and this is typically for archiving. The SSD portion is, in terms of latency, considerably faster. It is typically used for online data storage.

Samsung released their video: Samsung SSD Awesomeness almost five years ago now with the invention of the first SSD drives to demonstrate that if used as part of a striping RAID array there would be a significant performance benefit to the system.



Samsung SSD Awesomeness: <https://www.youtube.com/watch?v=96dWOEa4Djs>



# 1.8 inch versus 2.5 inch

For SSD, there are two different laptop form factors. Given the form factor considerations here it is clear to see that the 1.8 inch operates at a lower power and drive speed than 2.5 inch.







# Memory

We have previously mentioned that swapping memory on a laptop is not so easy as the SODIMM RAM is located with one slot typically below the motherboard (base) whilst the other slot is above the motherboard (behind the keyboard).

On phablets or smartphones the SIM card itself is the additional memory for the device, giving the end user the option to choose between onboard storage or storage on the SIM card.





# Smart card reader

A CAC or smartcard is an ID card used to identify personnel. It is the same shape and size and also functions similar to a credit or debit card. It contains a small chip on which a certificate file has been saved. This certificate holds identifiable information about the employee.

The smart card reader therefore allows us to use two-factor authentication (something you know that is password, and something you have that is the physical CAC card). This strengthens security and proves that the person using the laptop is actually the person they are claiming to be by logging on to their user account.



Not all, but a number of corporate-intended laptops (for example, ones typically using media or docking stations), if they do not have a CAC card reader may instead have a thumbprint reader to perform the same function. The main button on a Samsung Galaxy S6 or higher is in fact also a thumbprint reader, so access to your smartphone can be opened via thumbprint, or drawing a pattern on the screen.

Windows 8 was designed for touch-enabled devices and also supported pattern recognition. Here, a picture was presented to the user who had to touch or draw onto the picture. This was a good idea, but limited by the psychology of the human (for example,

if you are presented a picture of a face, touch points that would be obvious may be the eyes and mouth).



# Optical drive

Although most laptops have a built-in optical drive, as devices are manufactured with ever smaller and thinner form factors, optical drives are being phased out. As we may still need to access DVD-ROMs for installation, USB-connected optical drives are an option where one is not installed into the laptop itself.

Optical drives are used to access media (for example, to watch DVD films) and most laptop optical drives can also record CD and DVD.



# Wireless card

The ExpressCard is typically used to add a modem or wireless card. However, most laptops now have a dedicated mini-PCI wireless card attached to the base of the motherboard. The card is accessible through a panel in the base of the casing.







# Mini-PCIe

The Mini-PCIe slot supports both PCI Express and USB 2.0 standards and speeds. The form factor of the Mini-PCIe card is 30× 50.95 mm. Laptops built from 2005 onwards use Mini-PCIe; however, this is being superseded by a new standard, from 2015. M2 (Mini-PCIe v2) uses PCI Express v3 (4 lanes) and supports SATA v3 and USB v3, therefore it is ideal for a second internal hard drive.



# Screen

This section refers to material covered in section 1.10.

The laptop screen is made up of a lightbox (that is a hollow cavity with a backlight to illuminate the translucent screen) and the screen. All modern laptop screens are **Liquid Crystal Display (LCD)**. When electricity is applied to the liquid crystals, they illuminate as red, green, blue (or a combination of these adding up to white). The crystals overlap forming a pixel. The power to the LCD array alone however does not make the information on the screen visible--the backlight provides further illumination. This is typically a fluorescent light strip within the lightbox area to allow the user to see the information on the screen.

AC power is used to illuminate the backlight. However, where is this AC (mains) power coming from when a laptop is a mobile device, not connected to the mains? The laptop is powered by a power supply that steps down the voltage and also changing its nature from AC to DC. A low-power DC voltage is applied to the laptop battery that recharges but also conditions the incoming power where it is then used by the laptop components.

The florescent light within the backbox requires AC, not DC to function, so the process is reversed at this point. An inverter is a circuit board that is capable of creating AC power from DC, which then in turn powers the florescent light.

Average screen sizes for modern laptops measured diagonally across the screen, not taking into account the frame surrounding the screen. Dimensions are:

- **Ultraportable:** 13.3" inch or less
- **Thin and light:** 14" to 16"
- **Desktop replacement:** 17" to 19"
- **Luggables:** 20" and higher

There are two types of laptop panel currently in use.

TN panels have very narrow viewing angles (if you look from the side across at the laptop screen you will see a distorted, or even inverse image) where the light image is shone directly out of the screen. These tend to be cheaper and refresh rates (the speed taken to draw the complete image on the screen) is short. Screen color and brightness,

however, is poor in comparison to IPS screens.

IPS panels are more expensive, with higher color and viewing angles, but slower refresh rates. They are associated with use by Graphics Designers or Architects where high-quality detail is needed, but are not used by gamers or domestic users as the refresh rate is too slow.

Organic LED does not require a separate backlight--as the OLED is powered it also generates luminescence, not just color. Contrast and colors are much better from OLED in comparison with LED.



# DC jack

Laptops require power either from a mains supply or by battery. When connected to the mains the power supplied is used to also recharge the battery. Notice that mains power is AC and at much higher voltages (240V for the UK), so the job of the power supply is to step down the voltage and convert it to usable DC power.

Modern laptops (and this is certainly true with HP laptops as this has happened to me recently) also require that you use a manufacturer's own power supply. The reason for this is in fact security and ensuring that the warranty is met. This is policed by a data identification signal sent across from the power supply into the motherboard. If the identification signal is not found, the device will either not recharge the battery, or not power up at all.

Most electrical providers sell universal power supplies for laptops, which have a variety of DC power settings and jack connectors, however, you are advised to avoid these with modern laptops where the power requirements are exact and an ID signal is needed. Replacement branded power supplies are available and are sole for this reason, although they are slightly more costly to purchase in comparison to the universal power supply.

DC jacks tend to be proprietary to the manufacturer, with differing widths.







# Battery

Laptops are powered either by a mains supply connection, or by a built-in, but ejectable battery. There are three types of batteries used at present:

- **Nickel Cadmium (NiCad).**
- **Nickel Metal Hydride (NiMH).**
- **Lithium ion (Li-ion).** Li-ion is the most common.

When considering the efficiency of a battery, we look at the amount of power delivered in comparison to its weight (Watts/kg). We also look at the rate at which it will consume its power (Watts/hr), to full-discharge. We finally also consider the amount of times the battery is taken from a full charge to discharge (cycles) before it can no longer hold a charge.

The NiCad battery is cheap to replace and is quite stable. It is not prone to shock and recharges relatively quickly. It also has a high charge cycle. However, it is not as powerful as other batteries that have a higher power density.

NiCad contains metals that are non-recyclable; therefore they are not considered the best solution. They were widely associated with digital cameras and camcorders in the 1990s - 2000s, but are not the best choice.



Commonly used for games consoles and remote controllers, NiMh batteries store a low voltage, but are famous for their ability for recharging.

The concept of memory leakage for batteries refers to the fact that the laptop operating system makes a note of how full the battery is. However, this information may be wrong. If the battery is considered to be 50% full then it may only charge by 50% when in fact

it is empty and needs a full recharge. At what the laptop thinks is 100% charging may stop.

To counter this the advice is to completely run down the battery until it is empty, then fully recharge it, at which point the charge monitor will be in synchronization with the battery.



Charging memory issues are more prone to NiCad than to NiMh batteries. The batteries are made of environmentally friendly materials and are recyclable. The power density is up to 40% higher than NiCd. They are a simple battery and are easy to purchase as they are widely available. The problem is that they have a very short life-span and are very quickly discharged. They cannot be overcharged without damaging the battery and the charge time is quite long in comparison. If we use a fast-charge routine, or discharge them quickly then they will generate a lot of heat, which is not only a concern, but also will damage the batteries for future use.

The battery synonymous with laptop use is the Li-ion battery. These are the best for their power density. They are synonymous with laptops and mobile phones partly due to this very reason.

The Li-ion loses its charge naturally over time, which other batteries do not do. Other types of battery need to be primed (fully discharged and recharged before use) before they are put into service, however, this is not a requirement for Li-ion.

Li-ion batteries do not need to be fully discharged and recharged to reset the memory effect.





# Touchpad

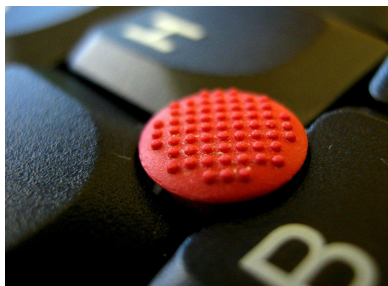
The touchpad is a finger-sensitive area below the keyboard on the laptop surface that acts as a mouse. The user drags their finger across the pad to simulate mouse movement. Most laptops have either one (Apple) or two (PC) buttons to simulate the mouse buttons.

The problem with the touchpad is that it is not as accurate, or easy to use as a hand-held mouse. Also, if the user rests their hands below the keyboard they may accidentally touch the touchpad, moving control from the window they are working on to another part of the screen, which can be quite annoying.

The touchpad requires a specialized driver provided by the laptop manufacturer to operate correctly, but most Windows systems support the touchpad natively, or by sharing the capabilities of the generic USB mouse driver.



Some earlier laptops, especially Toshiba systems featured a tiny finger joystick in the middle of the keyboard which also was used to control the mouse. It has a following even to this day.





# Plastics/frames

A laptop is made up of a display, the case frame (an internal metal chassis onto which the components are installed), and a surrounding plastic cover. The cover is typically made from a composite, lightweight, but durable plastic.

Frames are measured based on their width, depth, and height. The height of a laptop has been reduced greatly to now the thickness of the height of a USB cable, bringing the phablet into more common use.

We refer to the size of the laptop by the diagonal measurement from corner to corner across the display, in inches, for example, 17".





# Speaker

Speakers are built into the laptop, usually located at the base of the screen, or at the top of the keyboard. They are integrated into the main body of the laptop. An SPDIF jack is usually also available. These ports as sensing ports - once headphones have been plugged in an alert is given to the OS to mute the speakers and provide sound to the headphones instead.



# System board

The integrated mainboard has components on one side, but it is common to see that the laptop system board is of a shape allowing space for RAM, PCI slots, and the hard drive to be fitted. Internal ports are limited with one SATA port - the hard drive is fitted into a caddy and pushed back against the system board where both the data and power ports lock into place. The hard drive is then held into position, with the device in tension to the system board with a locking screw.

RAM is typically located with a port either side of the system board - one RAM slot is underneath the keyboard and one is on the base of the unit. Some manufacturers have two slots at the base of the unit, in the corner at an angle so that both can fit in the space provided. RAM is usually paired, so you have to add the same RAM cards into both slots.

The PCI express card is a universal port, commonly used to cater for a Wi-Fi adapter. There is just enough room to fit the adapter card and antenna. As with the hard drive, the card is held in place, in tension against the system board with a locking screw.

It is common to see that all ports and the graphics card itself are in fact on the surrounding daughterboard with the mainboard in the centre of this. This depends on the manufacturer - some split their boards and some have one large board.



# CPU

Central to the system board is the processor, which requires good airflow from the exhaust on the underside of the laptop. Laptop processors use the **Flip Chip Micro Ball Grid Array**, using balls rather than pins to establish connection to the processor. Lower voltages and clock speeds are used on the laptop to reduce heat buildup. Processor throttling is common on laptops as are more aggressive power plans.



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- <http://www.professormesser.com/free-a-plus-training/220-901/laptop-expansion-options-2/>
- <http://www.professormesser.com/free-a-plus-training/220-901/replacing-a-desktop-with-a-laptop-2/>





## **901.3.2 Explaining the function of components within the display of a laptop**

This section will focus on the characteristics of the monitor display, looking at the different hardware components used and considering where one display type may differ from another (for example, OLED is cheaper to manufacture, but the screen is not as clear as a backlit TN display).



# Types

We have already established that the hardware used in a laptop differs from a PC in that it is reduced in size and designed to fit in the smallest possible space, often containing on-board integrated components. This section will focus on the monitor hardware components and how they differ.

We will further explore other hardware components found within the laptop and laptop-specific peripherals (for example, Digitizer).



# LCD

As previously mentioned in 1.10, the laptop screen is made up of a lightbox (that is a hollow cavity with a backlight to illuminate the translucent screen) and the screen. All modern laptop screens are **LCD (Liquid Crystal Display)**. When electricity is applied to the liquid crystals, they illuminate as red, green, blue (or a combination of these adding up to white). The crystals overlap forming a pixel. The power to the LCD array alone, however, does not make the information on the screen visible - the backlight provides further illumination.

Average screen sizes for modern laptops are measured diagonally across the screen, not taking into account the frame surrounding the screen. Dimensions are:

- **Ultraportable:** 13.3" inch or less
- **Thin and light:** 14" to 16"
- **Desktop replacement:** 17" to 19"
- **Luggables:** 20" and higher



# TN versus IPS

TN panels have very narrow viewing angles (if you look from the side across at the laptop screen you will see a distorted, or even inverse image) where the light image is shone directly out of the screen. These tend to be cheaper and refresh rates (the speed taken to draw the complete image on the screen) is short. Screen color and brightness, however, is poor in comparison to IPS screens.

IPS panels are more expensive, with higher color and viewing angles, but slower refresh rates. They are associated with use by Graphics Designers or Architects where high-quality detail is needed, but are not used by gamers or domestic users as the refresh rate is too slow.





# Fluorescent versus LED backlighting

This is typically a florescent (**Cold Cathode Fluorescent Lamp (CCFL)**) light strip within the lightbox area to allow the user to see the information on the screen.

In order to manage brightness, **Pulse Width Modulation (PWM)** is used. The backlight is on for a certain period of time and is also off for a certain period of time. The light is effectively strobing. When you adjust the brightness setting you are altering the length of time the light is on and off. The earlier version, CCFL, does not react as quickly as LED to state change, producing a fading on the screen for a short time, where LED does not do this.

Test this with your own laptop by switching the monitor off and then back on. On laptops use Alt + Tab to switch between a full-screen black image and another app that is white and you will see that it takes a short time for the full brightness to be reached.



# OLED

Organic LED does not require a separate backlight--as the OLED is powered it also generates luminance, not just color. Contrast and colors are much better from OLED in comparison with LED. OLED devices are thin and highly portable.



# Wi-Fi antenna connector/placement

The laptop antenna is a coiled wire located in the corner of the laptop. Transmission range is not as large as a well-placed Wi-Fi antenna located on the back of a wireless NIC. Power usage is also often less than a standard PC wireless NIC, so the remote device has to be within good range of the receiving access point. As the device is mobile and the user will physically be roaming the network will more likely to be cellular in nature, meaning that, for example, a smartphone would connect to the nearest phone provider mast within a geographical area. A laptop would connect to its nearest hotspot. If you are traversing within an office building, or campus, the same SSID will be used by several access points and the device will connect to the strongest one (thereby the nearest access point). Access points are placed centrally within the building, usually on the ceiling. APs are omnidirectional and are strategically placed so that the best coverage for the room can be achieved without signal bleed through the walls, also with overlapping rings, so that the roaming device can seamlessly connect to the next access point without loss of connection.



# Webcam

The webcam is integrated into the top of the screen and can be switched on when required, controlled by video conferencing apps such as Skype. The webcam has to be calibrated for the lighting conditions, with a black and white-balance taken to ensure optimal recording of the environment. Modern webcams do this automatically at the start of the session, as the laptop will be constantly moved to new locations.





# Microphone

Next to the webcam is a microphone. On a modern laptop, as with the webcam this is muted by default and triggered when needed. The microphone is sufficiently distant from the speakers as to not get fold back (audio picked up by the microphone, fed back through the speakers where it is amplified until an audio squeal is developed). Again, it needs to be calibrated so that pickup from the user who is a standard distance away (usually about 1 meter or less) can be achieved.



# Inverter

AC power is used to illuminate the backlight. However, where is this AC (mains) power coming from when a laptop is a mobile device, not connected to the mains? The laptop is powered by a power supply that steps-down the voltage and also changing its nature from AC to DC. A low-power DC voltage is applied to the laptop battery that recharges but also conditions the incoming power where it is then used by the laptop components.

The florescent light within the backbox requires AC, not DC to function, so the process is reversed at this point. An inverter is a circuit board that is capable of creating AC power from DC, which then in turn powers the florescent light.



# Digitizer

This is a general term for what artists know as a graphics tablet. It is an input device accepting touches and gestures from a stylus/pen that are converted into movements and strokes. The Digitizer is commonly used by graphic artists when creating finely detailed images.





# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide.

- Laptop Displays: <http://www.professormesser.com/free-a-plus-training/220-901/laptop-displays-2/>





## **901.3.3 Given a scenario, use appropriate laptop features**

Laptops also have additional functionality not present on the PC and is specific to the fact that the device is in use at various locations. These additional functions can enable specific wireless connectivity, or adjust how the laptop is displaying its data.

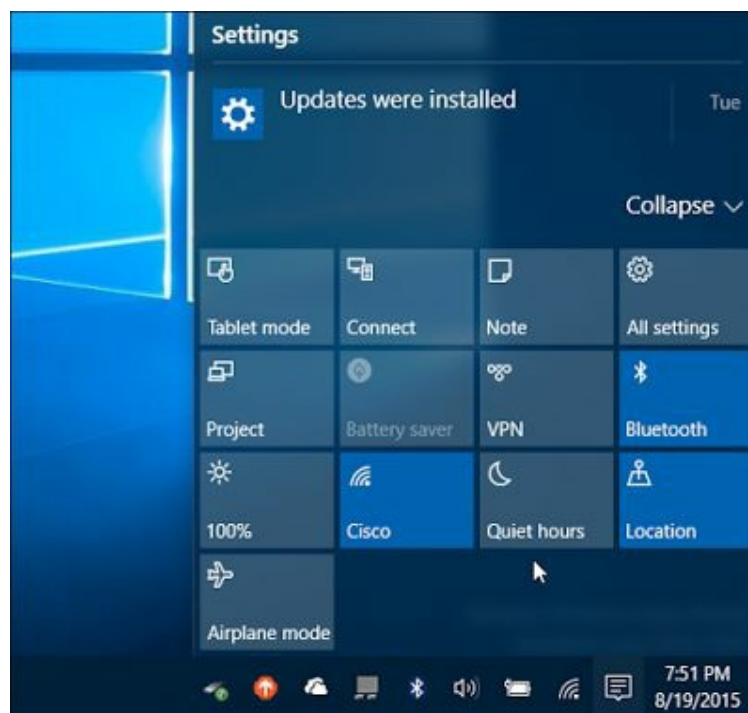
One key function of a laptop is to present information on more than one screen. Projection can be controlled by using a second virtual screen, or by duplicating the output on screen 1 through an external video port.



# Special function keys

Additional functionality specific to the laptop are controlled by an additional set of functions added onto the existing f series keys located at the top of the keyboard. Using the function lock you can access display controls, monitor brightness, volume settings, but also put the laptop into airplane mode, play media (for example, back, forward, play, stop):

- **Dual displays:** The OS has a project pane in which you can set the display to only monitor 1, or 2, duplicate the output from monitor 1 onto both, or extend the footprint. When in extend mode the order in which 1 and 2 relate to each other can be adjusted, so that extra space is on the right of monitor 1, or below, left, or top. Pressing the Dual Display button has the same function as the Windows key + P in that the Project Pane is displayed.
- **Wireless (on/off):** Separate to airplane mode, the Wi-Fi card can be disabled by turning the wireless function on or off. This is accessible through the soft buttons in Action Centre, or by using the Wireless key.



- **Cellular (on/off):** Also referred to as Mobile Data this is a paid-per-use service offered by the telephone provider, allowing access to the internet when a Wi-Fi access is not available. Where both Wi-Fi and Mobile Data are switched on, Wi-Fi will be preferred so as not to incur additional costs.

- **Volume settings:** For a laptop, the master volume setting is located on the Taskbar. By double-clicking you can get to a mixer desk where individual components volume settings can be changed. The master volume can also be raised and lowered by using the volume buttons on the device itself.
- **Screen brightness:** Rather than having to go into the display settings the screen brightness can be raised and lowered by using the brightness buttons. This function is also available from action center.
- **Bluetooth (on/off):** Where Bluetooth functionality is supported, the Bluetooth symbol (H and B in Nordic runes) is also available both on Action Center and as a function button.



- **Keyboard backlight:** To make it easier to see the keys on some laptops, also for aesthetic reasons the keyboard can be backlit with a neon light (for example, Alienware laptops). However, to conserve power this can be turned off.
- **Touch pad (on/off):** Many laptops have a touchpad located below the keyboard. For some users this can be problematic as their hands may accidentally press the touchpad and move the mouse whilst typing and moving the caret focus to somewhere else on the page. When using a separate USB mouse it is therefore preferable to switch the touchpad off, which can be done from this control.
- **Screen orientation:** Phablet and smartphones both have a spirit level device that determines whether the user is holding the device in portrait mode or landscape (tall or wide). The screen will redraw accordingly. This is useful when you want to display a video in full-screen and want to simply turn the display around 90 degrees.
- **Media options (fast forward/rewind):** As one of the main uses of phablets, laptops, and smartphones is to view video content, media buttons allowing direct connection to the media player in use are present allowing the user to skip or to replay a section.
- **GPS (on/off):** GPS and location are both used to allow GPS data from your phone, also to report back your current position. This is used by apps such as Google Maps that will then be able to triangulate your position and advise how far away a destination is, also to map a route for you to follow.
- **Airplane mode:** Similar to the wireless key, Airplane mode is also a separate key and will turn off all RF functionality. It was designed to allow the device to continue to be used whilst on an airplane. Again this is also accessible through

Action Center.

- **Docking station:** A docking station is a hardware component that acts as a base for a laptop. All cables and media (for example, DVD-ROM) are connected to and housed in the docking station. The laptop clips on top of the docking station making electrical connection through one common port on the base of the laptop. Once connected the laptop is considered to be 'docked' and the additional functionality is made available to the laptop.

For smartphones a common access port--Micro-USB is used to charge the phone, but also to use the phone as a media player.



- **Physical laptop lock and cable lock:** A Kensington lock is a barrel lock that attaches to the metal chassis frame within the laptop. This makes the device difficult to steal when locked in place. The cable lock can be used to tie a laptop to the desk.



- **Rotating/removable screens:** Modern laptops, such as the Surface Book have a detachable keyboard. In Action Centre once you press the detach button the attached green light will turn red and a click will be heard as the keyboard unlocks. In detach mode, the OS realizes the change and converts to tablet mode - open apps are full screen with no taskbar at the base of the screen. This is commonly used by graphic artists to be a creative canvas.





# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide.

- <http://www.professormesser.com/free-a-plus-training/220-901/laptop-features-2/>





## **901.3.4 Explaining the characteristics of various types of other mobile devices**

This section will take a broader approach to mobile technologies covering all aspects of hardware that are not laptops. These devices often serve a specific purpose (for example, tablets are designed to be an e-book reader, but can also perform all of the functions of a smartphone and some of the functions of a laptop). Their absence of a physical keyboard, however, makes them not as productive when it comes to data entry. The hybrid tablet/laptop such as the Microsoft Surface has a removable keyboard that when undocked triggers the operating system into tablet mode simplifying the user interface.

Our understanding is broadened to encompass these other specific-purpose devices that integrate the person with their data.



# Tablets

A tablet is a full-screen device used mainly for reading or web viewing. It can perform all of the functions of a laptop, and has an on-screen keyboard, but as there is no physical keyboard typing is much more difficult on a tablet.



# Smartphones

A smartphone's form factor is considerably smaller--a mobile phone first, and a tablet second. Both tablets and smartphones have a minimal, multi-purpose operating system capable of most of the features of a laptop, minus the keyboard.



# Wearable technology devices

We now extend our understanding into personal, wearable technologies. These standalone devices are designed to integrate wirelessly with a media server or smartphone so that data can be seamlessly shared. In the case of the smart watch or FitBit, geocache coordinate data can be uploaded as can your medical readings along with the distance you have walked on a recent journey.

Wearable devices are devices that can fit into the pocket but connect with the body, for example, Wi-Fi headphones or a watch that can measure your heart rate and steps you have taken.





# Smart watches

A smart watch is a combined MP3 player, watch, and some also feature a pedometer. They are used by runners and people interested in listening to music whilst keeping fit. They contain a GPS, compass, accelerometer, and gyroscope, so it can accurately record your movements.

Some smart watches can also be used as videophones, or standard mobile phones. The idea is that you have the functionality of an MP3 player and smartphone as wearable technology.





# Fitness monitors

A fitness monitor (for example, **FitBit**) is a type of smart watch geared towards fitness. The device, which as well as telling you the time, also is fitted with gyroscope, a GPS and pedometer, also a heart rate monitor. From this health and fitness data can be sent to a common profile, often this is stored in the cloud. You can use health data to determine your fitness levels.

There are different views as to the effectiveness of a FitBit. It is designed to encourage users to be self-aware and conscious of their health.

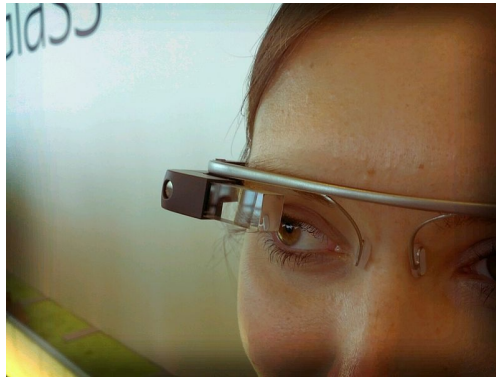




# Glasses and headsets

Sadly, the biggest flop of recent times was the Google Glass. This was a set of spectacles with integrated screen allowing you to see smartphone output on the eyeglass in a hands free format. It uses voice commands to be able to control features of the device.

However, due to safety and legal concerns the project was dropped.





# Phablets

Slightly larger than the smartphone and more analogous to the Kindle Fire, the Phablet has all of the features of a tablet, but also the functionality of a smartphone. It combines both functions into one device, allowing you to make calls and read on the same device.

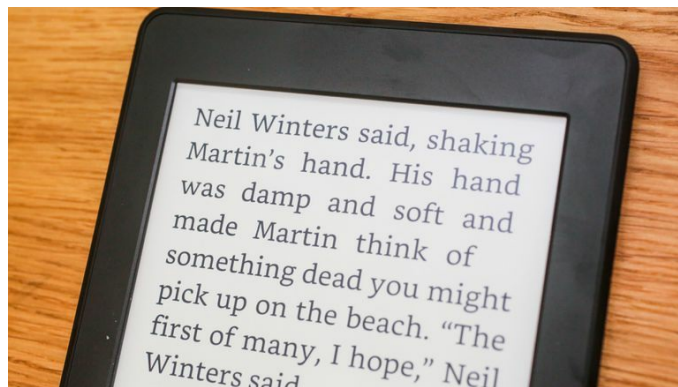






# e-Readers

Similar in size to the phablet, an e-reader started out as a dedicated e-book reading device. Later models came with color and full Wi-Fi connectivity, and even were comparable to tablets. With the Kindle Fire the definition is blurred - it is now capable of all actions also capable on a tablet. However, traditional e-readers such as the Kindle, Paperwhite, or Kobo are dedicated e-book readers allowing you to view a book, page by page, in full screen.





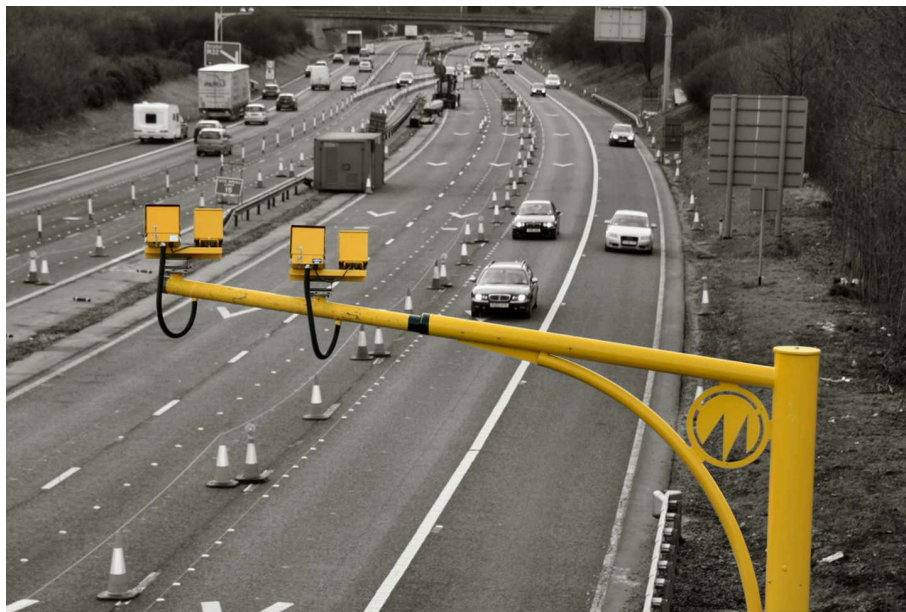
# Smart camera

The term Smart Camera actually defines two very different technologies:

The digital camera with Wi-Fi capability can transfer files to the cloud or to your PC across a personal area network (Wi-Fi or Bluetooth) for storage for further editing.

Secondly, the smart camera can also refer to motion-sensing CCTV, internet-enabled cameras used for home and small office used to record movements as part of a passive security system. Yale, Swann, and Lorex are common modern intelligent CCTV suppliers.

One further important use of smart cameras is their application with factories and also on motorways and highways. In factories, objects on a production line belt can be checked using pattern matching and edge detection to check for defects. For the motorway, smart cameras are used for **automatic number plate recognition (ANPR)** to check that the vehicle is licensed and taxed. They can also be used as speed cameras, recording a digital image and by comparing two images of the same point against a speed grid on the floor the exact speed the car is travelling at can be determined and results sent back to a collection server (modern GATSO system).





# GPS

The **Global Positioning System (GPS)** uses an array of satellites spanning the globe that measure the distance to up to four satellites in orbit. This is used to calculate coordinate data exact to up to 2.5 square meters. A GPS device is a watch with GPS functionality. For parents concerned with their child's safety, but where smartphones are banned in schools GPS watches provide an ability to track the movements of a child who may abscond, or go missing. They are also common with GeoCachers--people interested in combining walking and mapreading to find clues and treasure.





# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide.

- <http://www.professormesser.com/free-a-plus-training/220-901/mobile-devices/>





## 901.3.5 Comparing and contrasting accessories and ports of other mobile devices

In this section, we will look at the wireless connectivity components we can use to extend the device, also to share data across a **Personal Area Network (PAN)**. We are going to go broader than the typical mobile covering a variety of smartphones and even games consoles.



# Connection types

We start by considering the various types of non-wired connection from a practical aspect - how are they used and why these connection types are specifically used. We will look at newer techniques (for example, NFC for payments), also the practical advantages of some of the connection types (for example, the use of Apple's magnetic pins to hold the power plug in place.)



# NFC

Near-field communication is a low-range, low-power RF signal sent to a receiving device. Common uses are to print directly to a print device direct from a smartphone, also to pay for goods and services in a retail store. The Apple iPhone 6 and smartphones with Google Wallet installed can support NFC payment to a wireless-enabled terminal.

In order to use it, simply hold the phone close to the terminal until an approved message is noted on the terminal.





# Proprietary vendor-specific ports (communication/power)

Some vendors provide specific ports unique to their device. For example, if we consider the MacBook Air or MacBook Pro we will encounter a range of non-standard ports, but first I want to draw your attention to MagSafe. This is a charging port used on modern MacBooks with a series of magnetic pins making the connection into the socket. If a passer-by knocks the power cable, the cable will be pulled out, but as the charging socket is not locked in place it is unlikely that the MacBook will also be pulled from your table. The MagSafe port will be replaced in later models, but it was an interesting port nonetheless.







# MicroUSB/miniUSB

At the time of writing, the Lightning port is in the process of being replaced on Apple devices by microUSB. This is as a result of a ruling by the European Parliament's consumer protection committee in order to standardize smartphone connectors, to reduce waste and to simplify device usage. The MicroUSB port is a generic port for data transfer and device tethering, but is the main charging point for the device.



# Lightning

Apple's lightning port was found in the iPhone 5. It replaces the earlier 30-pin port, but this move was unpopular with Apple users who already owned the previous version Lightning-connected products and did not want to update. Lightning offers more functionality than standard microUSB, such as the fact that you can directly control accessories from the iPhone screen from another device over this port.

The main use of the Lightning port is to connect iPhones, iPads/ iPods to a host PC or to other external equipment such as external monitors, cameras, and USB battery chargers.





# Bluetooth

As described earlier, Bluetooth is used to directly send to another device within 10 meters and has replaced infrared as a direct PAN communications method. The devices have to be paired and the connection is secured with a 4-digit PIN code. Bluetooth is also now synonymous with headphones and to connect a Fitbit to a smartphone to upload health data.



# IR

There are problems with Infra-red:

- You need a direct line of sight from the transmitter to the receiver
- The range can only be sent within a distance of 1 meter approximately.
- Data transmission is slow in comparison to Wi-Fi or Bluetooth

However, as with Bluetooth, this is a low-tech solution as it requires no further equipment or cabling, in contrast to Wi-fi that does require an access point.





# Hotspot/tethering

What we tether to has changed - tethering traditionally is the sharing of mobile data across a dedicated RF channel, or cable, such as a USB cable. Now, with the focus on wearable technology, we are extending our smartphones to our bodies (for example, smart watches and headphones), making the smartphone effectively an access point for your peripheral, wearable devices, allowing real-time upload of data, or for example the streaming of music to the device rather than transferring data whilst offline (for example, in previous years an MP3 player would need to have the required songs copied over onto the device from a media server or host PC. Now the entire library can be stored on the smartphone and a playlist streamed to the headphones via Bluetooth).



# Accessories

We have already started to introduce the fact that the smartphone is now considered to be the host PC for those of us on the go. The peripheral is often not an extension of the PC in the way that a printer is separate, rather is a wearable commodity, often providing sensory input or stimulus to the user.

Of course the downside to this expansion and propensity of tech is that there are more devices you need to charge.



# Headsets

Wireless headsets typically use a dedicated Bluetooth channel - music is streamed to the headphones, which are portable, lightweight, wearable, and integrate well with the user.

Whilst on a technical level this is good, there are fundamental social concerns around the individual shutting off from the rest of society as the individual draws back into their own world and ignore some of the world around you. This is a clear safety concern for pedestrians when crossing a road, or simply walking next to another pedestrian as they are not focusing on what is happening around them, or engaging with others.

We are starting to see a paradigm shift on the personalization of self and it is an interesting note that the more tech we wear the more we are distracted by it and live in our own artificial worlds.



As with headphones, Bluetooth speakers eliminate the clutter of wires and provide good quality audio from small speakers that are often powered by a rechargeable battery.



# Game pads

A game pad is designed to react to fast user actions such as joystick movements, or trigger presses. Designed with action or sport games in mind, the user holds a two-handed device molded around the normal grip of the hand. Taking the X-Box 360 control as an example you are presented with two trigger buttons, two select buttons, two joysticks, a compass joystick (known as the Directional Pad), and four control buttons. There are two additional buttons to access game menus and the main X button designed to turn on/off the controller.

The controller also features a 2.5mm TRS connector where you can plug in a wearable headset, used when playing online team games.

The game pad also provides tactile feedback to the gamer with a built-in vibration device. If the user, for example switches on an engine and is in the proximity of the engine, or is flying a helicopter, the vibration is felt through the hands, providing a more realistic gaming experience.

Game pads are either wired, connecting through a proprietary game port to the console, or are wireless. The controller can be wired to the console by either the USB or microUSB ports.







# Docking stations

Most docking stations are now also sound bars--a stereo speaker set built into the docking station and offering high-quality, high-definition surround sound. These are popular for living-rooms and kitchens replacing the traditional Hi-Fi, or kitchen radio - the use has not changed, but the technology has improved.





# Extra battery packs/battery chargers

Battery life and the holding charge time has improved considerably, however, there may be times when you need to continue to use the device, but the battery is running low. As USB can send power, portable power banks are an additional charged battery that can be used as an alternative power source, or to charge up your phone whilst away from your charging station.





# Protective covers/water proofing

Smartphones in particular can be contained within a silicone / plastic protective case. The case is molded to the specific model of the phone as most have different dimensions and relative positions for their camera and buttons.

The protective cover is translucent and allows the user to interact with the phone in the normal way. Touch is not affected.

The cover protects the display from smears, dirt, or scratches, but also offers a limited degree of water damage from rain.

Modern smartphones are now sold on the premise that they are completely waterproof with the Samsung Galaxy S7, S7 edge, S8 and S8 plus, the LG G6, and the Apple iPhone 7 are all water resistant.





# Credit card readers

Credit card readers support wireless NFC from contactless credit and debit cards, also from your smartphone if the Google Wallet or similar app has been installed.

There has been mixed reviews of this service, with older non-users reluctant to convert over concerns that, in the case of use of NFC within debit cards, one might walk past the person in front of you in the queue and inadvertently pay for their shopping. This is of course nonsense due to the duration and proximity of NFC.

Restrictions are in place on the use of NFC - depending on the retail outlet there is a payment cap of £20 / £30 and the service can only be used a few times per day to prevent fraud, or theft from the account. Once NFC is blocked the owner has to present the card in the normal way and use Chip and PIN to complete the transaction, as a security check.







# Memory/microSD

In addition to on-board memory, smartphones have a port to accept a MicroSD card located next to the SIM/microSIM card. This provides effectively a second hard drive and provides the user with an option to archive their files onto the SIM card where it can then be shared with other SIM-compatible media, or transferred onto a PC with a Media Reader fitted.

MicroSD cards are now typically 64/128GB in size (and even larger), so support a large archive of personal media.



# Exam questions

1. A Windows 10 user wants to know how they can turn their Surface laptop into a tablet. They have tried to physically remove the keyboard but it will not come apart. How can you advise them to convert their laptop into a tablet?
  - Answer:
2. A Windows 10 user tries the advice given in the question above however the keyboard will still not detach. Can you think of a reason which this might be?
  - Answer:
3. The Expresscard 54 accepts which types of card?
  - Answer:
4. Which type of hard drive is least susceptible to damage or data loss if accidentally dropped?
  - Answer:
5. What is the function of an inverter card?
  - Answer:
6. What additional keys located on or near to the function keyset can be used to control media player applications on the laptop?
  - Answer:
7. The user connects an external monitor to their laptop however the screen remains blank. Why may this have happened and how can it be resolved?
  - Answer:
8. Your customer is concerned about physical security. They have a series of laptops on public display and do not want the device to be easily removed. The devices have to be used by members of the public, but not taken away from the desks. What would you suggest?
  - Answer:
9. What is the primary safety concern with internet-enabled glasses which led to their withdrawal from sale?
  - Answer:
10. A sales representative has attended a conference and is now back at the hotel. The representative cannot connect their laptop directly to the hotel wi-fi as the signal strength is poor. However, she was able to use her mobile phone to connect to the internet and use her laptop anyway. What technique is being described here?

- Answer:



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide.

- **Mobile Device Connections:** <http://www.professormesser.com/free-a-plus-training/220-901/mobile-device-connections/>
- **Mobile Device Accessories:** <http://www.professormesser.com/free-a-plus-training/220-901/mobile-device-accessories/>





# Summary

So to conclude, we have seen here a large collection of components specific to mobile devices, tablets and phablets. We first looked at laptop expansion slots across the years, then how we could replace a keyboard or to add additional storage. We then looked at the broader components which make up a laptop and which differ to the PC, such as the frame, the uniqueness of the laptop system board, power requirements and other hardware differences.

We then turned our attention to the types of display available for the laptop, followed by other hidden components which as the wi-fi card and antenna, microphone, inverter card and camera.

We then considered specific situations where you may want to make use of some of the additional features of the device, now broadening out to include smartphone and phablet features such as adjusting the screen orientation, or to switch additional functionality such as wireless, Bluetooth or sound on and off. We then considered where corporate laptops can be docked and undocked from the connected docking station and in undocked mode can connect to the corporate network wirelessly, or to an alternative network if used at home. We also looked at security devices such as a barrel / Kensington lock and hardware enhancements such as the removable screen (for example, on the Surface laptop) at which point the OS swaps modes and it works just as a tablet.

In the broader sense we then compared different mobile devices and also considered wearable devices such as a Fitbit, GPS, or smartwatch. Finally we then looked at the wider family of supporting devices associated with mobile systems including headsets and gaming-ware but also connection types used by these to connect to the mobile system.

Overall, this chapter has expanded our association - IT Technicians now not only support PCs and laptops but wider devices which share data with them. This is now reflected in the A+ course and exam.



# Hardware and Network Troubleshooting

## (901.4)

You are about to embark on one of the most important sections of not only this book, but your entire career. It is important that you consider not just the fact that you might, in the short-term want to fix a PC, but that the PC is often part of a wider corporate network and problems can exist on the network, rather than just on the PC alone. As far as your career is concerned there are two things you need to consider--(i) you need to act in a professional manner when dealing with customers and this goes hand-in-hand with good, concise technical expertise, and (ii) you need to adopt a troubleshooting methodology that also encompasses your understanding of networks.

Beyond the A+ course your next immediate goal is either to complete the Network+ and Security+ courses, thereby proving your experience at troubleshooting across an Enterprise network, but also demonstrating that you can keep the company safe. A+ only goes so far to doing this by focusing on the individual PC and its security and data movement. You may also consider vendor-specific certifications such as the Cisco CCNA, or the Microsoft MCSA as your move to second line support will be Swift. You are half-way up the mountain and A+ in itself is merely part-way along the journey.



# **901.4.1 Given a scenario, troubleshoot common problems related to motherboards, RAM, CPU, and power with appropriate tools**

In this section, we are going to focus on common problems you will encounter within the PC. We are starting by concentrating on symptoms common to an individual PC and these could affect any type or style of PC. You will notice that a number of these problems are hardware-related, that is around the four key hardware components of RAM, CPU, Hard Drive, and Power, but not the NIC yet as we cover network problems in a later section.



# Common symptoms

A great number of problems that can occur are due to instability. Instability can be caused by:

- Power loss leading to components not functioning which then causes the OS to become non-responsive
- A lack of free memory as data used by an app is not unloaded from RAM once the app is closed; leading to a situation where there is no free memory at all and the OS cannot cope
- Heat issues causing the system to throttle the processor, slowing down the PC and affecting performance
- Severe heat issues causing the PC to automatically restart

Most problems cannot be anticipated due to the preceding factors, or environmental factors; however, poor PC maintenance during a repair can lead to more immediate problems. For example, if you as a technician forget to power the fans within the chassis good intake and exhaust airflow will not take place and the heat will build up within the case. A more immediate problem is if you forget to reconnect the power to the CPU fan as the CPU will literally bake in a few seconds, destroying a vital component and probably also the motherboard as well in the process.

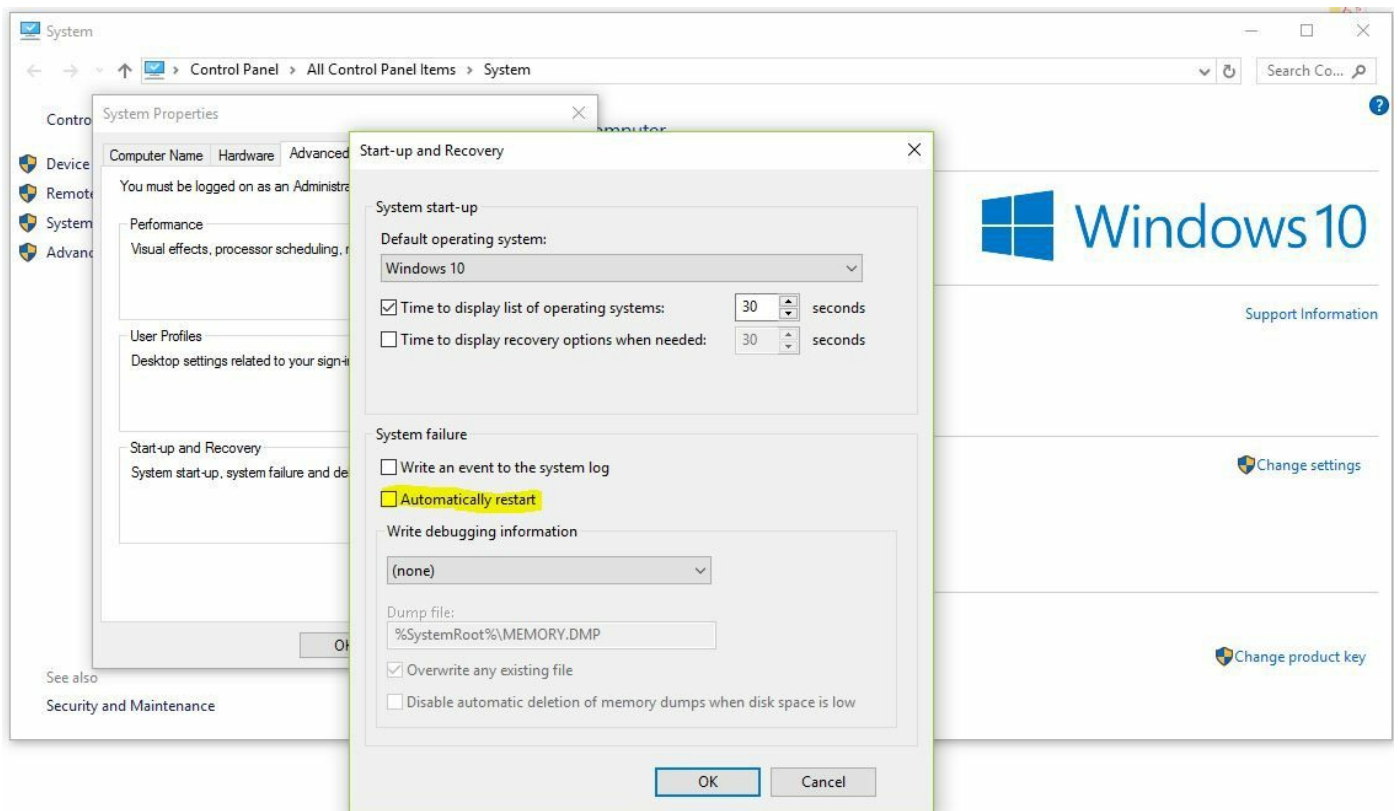
This section looks at a variety of problems, whether they are environmental, or ephemeral, or more immediate due to human error.





# Unexpected shutdowns

In order for a system to shutdown it needs permission to do so. By default, this permission is given in the form of the automatic shutdown box. A shutdown is triggered when an application becomes unstable but the underlying OS software is also affected. Normally the OS can restart the damaged service without causing the need for a restart, but if severe a restart will clear the problem. The problem is that if you have any unsaved work open, this work will be lost, so it is often better to clear this checkbox, encouraging the user to manually restart the PC instead.





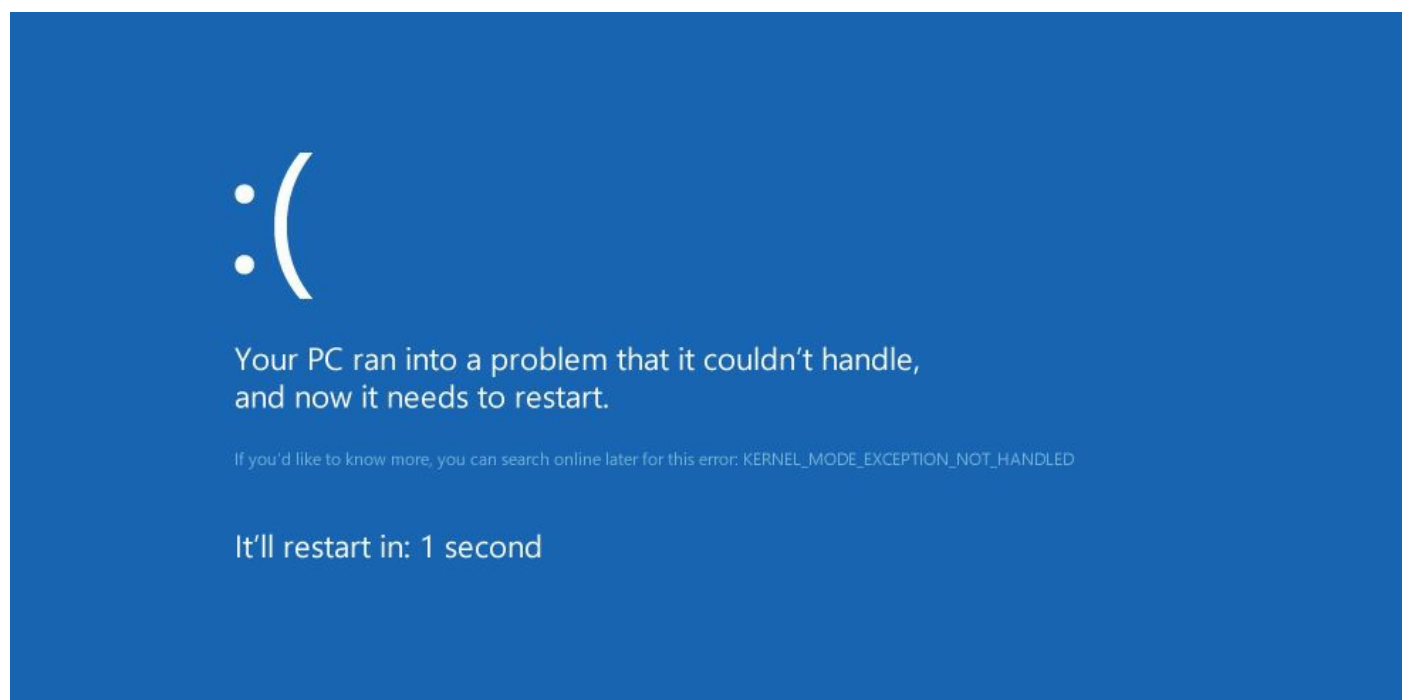
# System lockups

The system can become completely unresponsive when in-memory data key to the OS core system is damaged, or inaccessible. This can occur if an application has managed to write its own data over existing data needed by the system to function. Usually system address space is kept separate from application address space although this problem can happen.

Where hardware is also affected it can lead the system to hang. At this point it will pause, stop receiving any new input, and display an error message on the screen (known as a Blue Screen of Death). This indicates the location in memory where the fault has occurred.

As a developer, if the system hung while you are testing an app, you can ask the system to perform a memory dump of the exact data stored in the affected area of memory so that you can analyze this later on, once the system has been restored. To most end users this data is meaningless and requires expert debugging skills to be able to understand what has happened to cause the problem. Typically, on a standard SOHO PC debugging can be turned off.

Here we can see the Blue Screen of Death on Windows 8/8.1/10 systems:



Here we can see the older BSOD screen found on XP, Vista, and 7 systems:

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The problem seems to be caused by the following file: SPCMDCON.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xFD3094C2,0x00000001,0xFBFE7617,0x00000000)

*** SPCMDCON.SYS - Address FBFE7617 base at FBFE5000, DateStamp 3d6dd67c
```



# POST code beeps

The **Power-On Self-Test (POST)** is an initial electrical connectivity test made by the motherboard to locate and acknowledge the presence of a processor, RAM, and a graphics card. Success at this stage results in an audible short beep provided by the system speaker (on IBM systems). Each manufacturer has their own distinctive beep codes and you will need to consult the provider's manual to determine the fault. Other morse-code-style beep codes determine specific problems with the system.



A good resource to check these is <http://www.bioscentral.com/>.



# Blank screen on bootup

This is a common problem with DVI ports (as the trigger signal does not auto-switch the input selection on the monitor to the active port), but equally can be caused by an unseated video cable. Most commonly the monitor, which often has several different input ports, is set to look at the wrong input, so using the front panel buttons on the monitor you can switch over to the correct input port.

On initial startup the graphics card's ID, then the POST result and BIOS data are sent to the screen using EGA/CGA mode. The graphics card is able to send this data natively to the monitor without the need of an operating system at this stage. For this reason we can eliminate the OS and OS drivers.







# BIOS time and settings resets

AMD Athlon, Duron and Intel Pentium 3 and 4 systems motherboards had common problems when facing power cuts. Some end users wrongly turn off their PCs without letting them shut down gracefully. This can cause damage to the hard drive and means that the OS will take longer to start next time as it tries to perform tests and potential repairs to data stored on the hard drive, but more seriously there are cases of the BIOS configuration setting reverting back to factory default settings.

If the processor operates at a higher frequency to the factory default setting (the speed at which it was running when the OS was installed and the initial hardware audit was run), the OS may think that the hard drive has been removed and placed into a similar PC causing product activation to start. The OS will certainly re-perform a hardware audit and make configuration changes to allow the system to start, however the system performance will be greatly reduced, or the system may not start at all.

This can also happen if the BIOS reset jumper is cleared, or the lithium battery is removed from the motherboard (or has run down).



# Attempts to boot to incorrect device

Over time and use it is possible that the user has dual booted the system, installing multiple operating systems onto different partitions, even addition additional hard disks each with their own **Master Boot Record (MBR)** and Boot Configuration database. The starting point is with the Boot Order in the BIOS - the first hardware device is checked - if no boot information is found the next is tried. If this order is incorrectly set an older hard drive may be loaded from which in turn will load the wrong boot order. If no boot information or MBR is found the missing operating system message will be displayed meaning that no operating system was found on any drives.



The most common boot order is:

1. CD-ROM / DVD-ROM: This allows a technician to perform offline repairs or updates if disconnected from the network.
2. PXE Network boot: This allows the machine to receive a new image if it has been designated for a refresh. If it is not in the refresh list PXE will cancel after a few seconds and the next boot order tried.
3. Hard drive: As no disc is in the DVD drive and the machine is not on the PXE list, it will boot normally.



# Continuous reboots

This is most commonly found during the installation of a service pack, or critical update onto a system whose hardware cannot support the new code. The new code will try to run, fail, and the system will try again to install and test the patch.

Windows 8 systems and higher intelligently keep a counter as to the number of times the patch has been applied. If the number is over a threshold (for example, 2) then the installation will roll-back to the previous stable driver / code.



# No power

Most often the mains fuse in the kettle lead is to blame. Start your troubleshooting from the easiest point, that is the mains socket - is there a power switch on the mains socket? Is it on? Can the socket power other devices? Has the mains fuse in the plug blown? (Try another known good kettle lead). Next check the **Power Supply Unit (PSU)** - does the PSU have a power switch? Is it on? Is there a power light to prove power is being received? Is the input selector switch set to the correct voltage?

Within the PC you will notice a power LED on the motherboard. This provides power when in power off state. If this is not lit then it implies that no power is getting to the motherboard.

It could be that the P1 connector is unseated but this is uncommon because the P1 has a retainer clip to ensure a tight connection into the motherboard. Has the power button header wire become unseated? If you clear the 'wake' pins on the header does the system start up?

Potentially a multimeter would help here - you could test for power against a free molex plug, however please be careful with this and take electrostatic safety precautions.





# Overheating

The main concern is that if a core component temperature rises to above tolerance this may be caused by an overworking server. If the server is conducting a role that causes the processor to overheat, common practice would be to enable throttling on the BIOS of the machine. Throttling reduces the power and therefore the performance of the processor as an overworked processor generates more heat as the processor is required to work at full capacity. By throttling this gives the cooling system sufficient time to reduce the local internal temperature and specifically that of the overheating component. Without throttling, the PC will at first reboot. On a server this is dangerous from a business process perspective as services will be shut down and data will probably be lost. It will also take several minutes of remediation and restarting of internal services before all provided services are available once again. To help with this business service servers are clustered to ensure High Availability. On some systems, the server may shut down completely and suddenly if the core temperature of the CPU exceeds tolerance. Here again the danger is that the shutdown may lose data and leave the system in an unstable state as shutdown was not achieved in a graceful manner. The rebooting system will need to repair any file system damage as well as to reactivate all necessary services before the server is usable again.



# Loud noise

An unusual loud noise often suggests an obstruction to the chassis or processor fans (often a buzzing or sawing sound). With good cable management all data and power cables should be cable-tied to the chassis rails and out of the way of any fans, also ensuring good airflow. However, messy home-built systems may have loose wires snaking across the case in which case it is easy for these wires to come into contact with the fan blades. Over time this may cause damage to the fans which could burn out if stopped by the wires.

Certainly a loud noise would suggest that wires have moved and moving the chassis may temporarily stop the problem; however, you should power down and inspect for a fault.



# Intermittent device failure

If a device often works, but then in some circumstances stops working that could suggest either loose power, or that the system is underpowered. This is common with DVD-ROM drives when they require more power than the PSU can supply to the complete unit.

Other intermittent problems may be caused by equipment interfering with other components (for example, a cordless phone, or microwave generate RF interference on the same bandwidth as is used for Wi-Fi, so if the Wi-Fi router was next to such a device, when the device is in use users cannot connect to the Wi-Fi, which will drop out).

One recent example of this was an elderly lady who has a wireless emergency alarm system. If she were to fall, she could press the red button around her neck, which would trigger an emergency response team to check if she is OK. She also has internet Wi-Fi access and her devices connect on both the 2.4 and 5 GHz bandwidths. Devices using the 2.4 GHz cut out periodically.

Failings in the firmware can also cause the device to become unstable. These are often fixed in later versions of the firmware, so a software update will normally cure this.

If the device is overheating, once the processor gets to a set temperature the device will either throttle the processor, reducing the processing overhead to in turn reduce the heat being generated, or restart the system and by so doing clear any applications that were processor-intensive, allowing the system to return to a stable state.

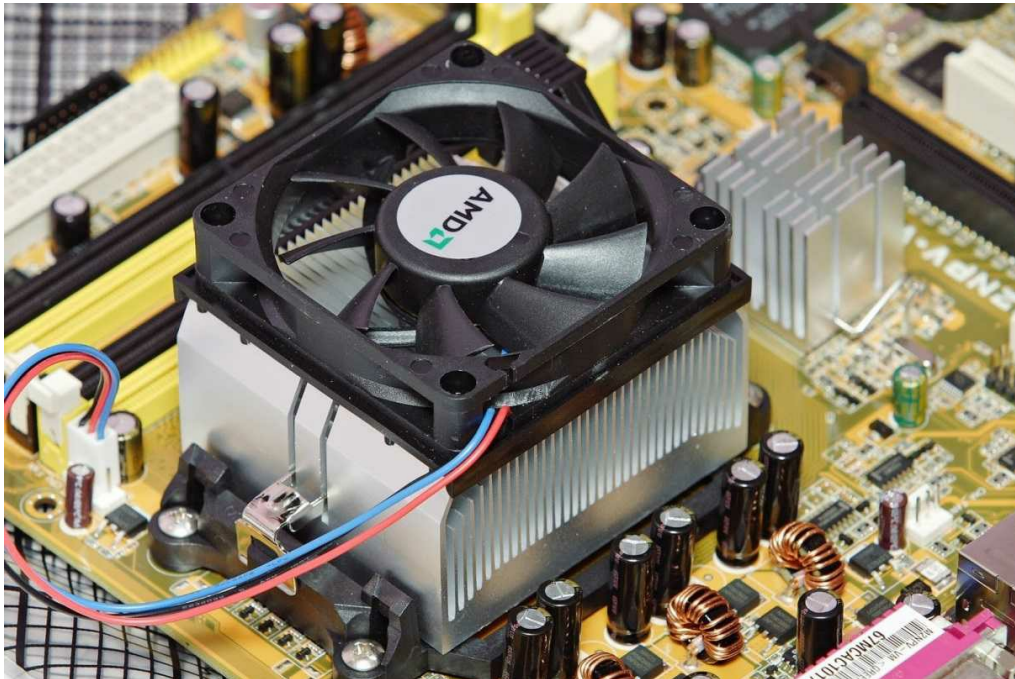
If the reset is triggered when a particular component is accessed it can imply a fault, or damage to that component only. An old example is a Windows 95 system with both a modem and audio card fitted. Both share the same **Interrupt Request line (IRQ)** and if a modem call was made whilst the audio card was still working the system would lock-up with a BSOD message. By changing the IRQ on one of the devices this could be overcome.



# Fans spin - no power to other devices

Fans spinning is usually a good sign, but POST is not a sure-fire test. On some systems the fans are hard powered meaning that power is supplied directly from the PSU that may be working fine, therefore it is not confirming that the motherboard is working at all. A BIOS firmware upgrade that has gone wrong (interrupted mid-upgrade) would cause a situation where POST cannot be performed which will explain why no beep code has been heard.

Modern PC systems are soft powered - power for at least the CPU fan is supplied from the motherboard, so if there is a fault with the motherboard power will not be transferred to the other devices, or fans.



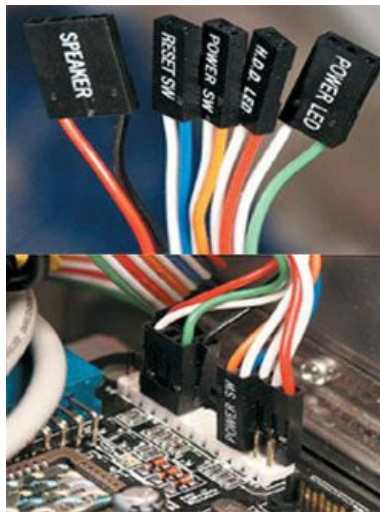




# Indicator lights

The chassis indicator lights, upon power-up should go into 'test' mode, meaning that the LED will light briefly for up to a second, and then clear. As power proves that the system is now in powered soft wake state, the light will be lit continuously. The Hard Drive light proves when the drive is being accessed, so it will flash only when read/write operations are occurring.

If no lights illuminate this could imply that the header wires from the LED to the header block are in fact the wrong way around. Whereas this is not a problem for the speaker, Light-Emitting Diodes are diodes - electricity will only flow one way. Some universal chassis providers have the header wires as separate plugs, whereas chassis manufacturers who make units specific to a particular motherboard type have a front umbilical header wire loom terminate in a specifically designed plug that connects all of the front header items in one go.





# Smoke

A very bad sign will be smoke coming out of the vents. This indicates whether a burning foreign object (for example, paper) inserted into the chassis has caught fire, or worse - the voltage regulator switch on the PSU was set to EU/US setting and as a result over double the expected voltage has just burned out the capacitors in the PSU.



# Burning smell

If the latter, you will hear a large bang as the capacitor explodes. The smell of burnt solder (a little bit like the smell of gunpowder) will be noticed. You may also smell tin from the solder as they overheat and liquefy.

It is essential that you make the area safe immediately. Remove any persons from the equipment and then cut the power to the area before attempting to tackle the smoke. Take precautions to not inhale the smoke that will be toxic.

Another occasion where you may smell burning is if the heat sink processor fan is not powered. The system will boot up and work for a few seconds until the processor gets so hot that it actually melts. At this point the system may be quieter than usual, but it is not so easy to notice that the processor fan is not spinning, especially on ultra-quiet systems. It is important that you cut the power immediately to stop melting solder from causing a short. To remedy this, depending on the extent of the damage you may well need to replace the motherboard, you will certainly need to replace the processor, but before all of this it would be advisable to check to see if power is still going to the fan power connector pins as the fault needs to be identified as either the fan itself or the motherboard.

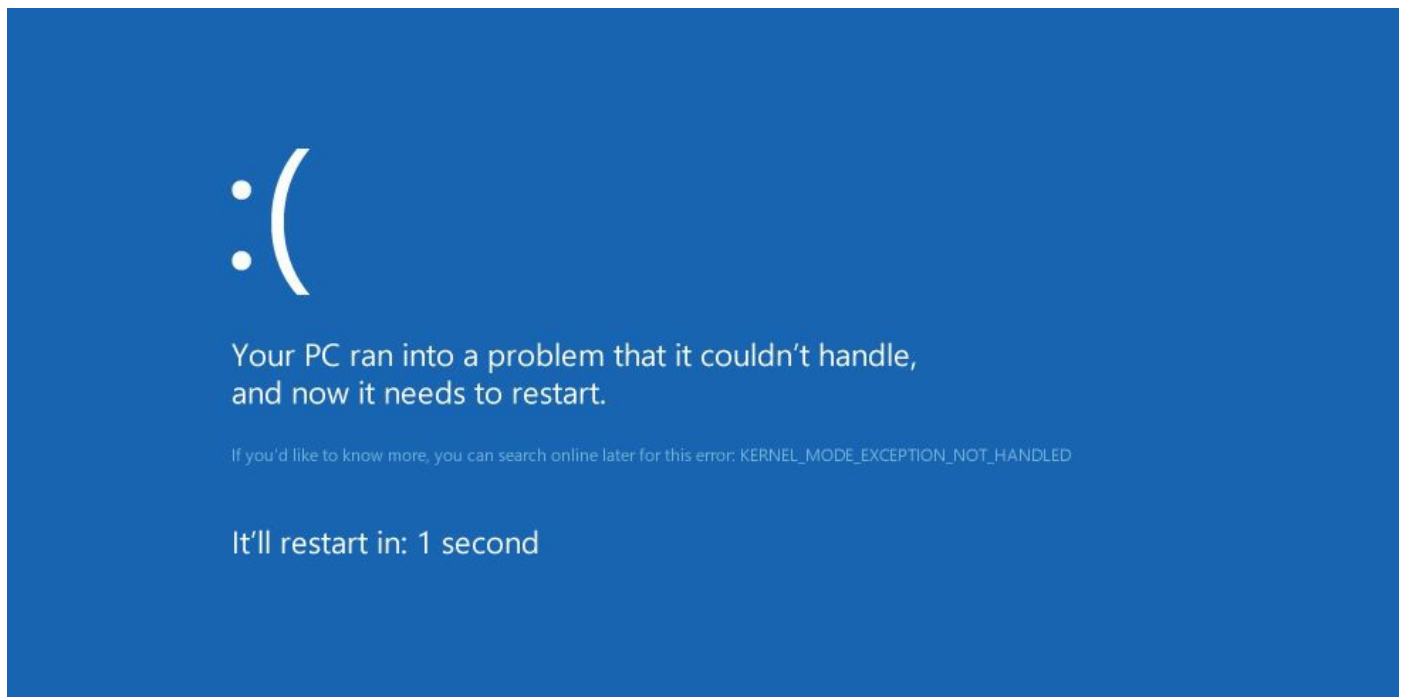




# Proprietary crash screens (BSOD/pin wheel)

The crash screen indicates that the system has become unstable and the data stored in RAM cannot be retrieved. This is usually caused where data in RAM has become damaged, or a section has been written to by a module or application and stored the data in a location it should not have done, which is in fact in use by another process, causing that process to fail. These are commonly found when changes are being made to hardware components, or the system is installing new hardware.

If the hardware is old (for example, installing Windows 8 onto a 32-bit architecture AMD Athlon system) and typically no longer supported then this can occur during a hardware audit during OS installation.



Apple's equivalent, the Spinning Beachball Of Death (or the pinwheel) is similar to the blue Windows spinning circle - it indicates that an application or module is trying to load, but is taking some time to do so. With Apple, the wait time is lengthy and usually you would have to manually kill the task from running, done with a `TaskKill` command.





Wait timers and pinwheel's, however, are recoverable - the system is still stable and it is only an app that is refusing to load, whereas the Blue Screen is much more serious and will require a system restart.

The extreme example is the **Spinning Pinwheel of Death (SPOD)** described in a later section. Here, the pinwheel is present for a long time, but in fact the system has halted.



# Distended capacitors

On visual inspection if a capacitor looks lopsided, or the top of the cap looks as though it is about to burst, it could imply a heat issue with the capacitor. Some capacitor manufacturers between 1999 and 2007 used impure chemical components (an electrolyte mixture used within the capacitor can) or were badly made leading to corrosion and gas buildup, causing the top of the capacitor can to burst and for the electrolytic compound to be spread across the motherboard, in some cases catching fire.



# Tools

In this section, we are going to take a look at a variety of tools used to perform repairs on your PC. I have also included some low-level tools you can make for yourself for a few pence (such as the loopback plug) that are useful for testing the physical NIC beyond what we can do through software tools such as `PING` and `IPCONFIG`.



# Multimeter

A multimeter is a simple way of testing for electrical connectivity between a component within a system (for example, across a fuse or resistor), but it can also be used to give an accurate reading for current, voltage, and resistance of a circuit.

A resistance of infinity would infer a connectivity break at this point in the circuit suggesting that a component would need to be replaced.

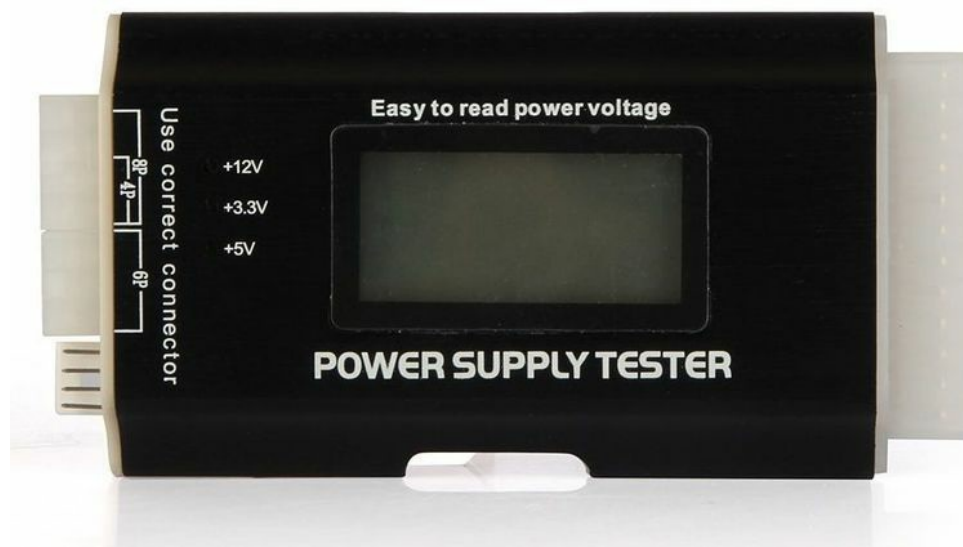






# Power supply tester

It is a legal requirement for companies to have their equipment power tested on a regular basis through a process known as **Portable Appliance Testing (PAT)**. Here, the device is subjected to a safe test through sending different loads within the power rating of the device to check that the device is able to handle differences in power. It is also possible to use a Power Supply Tester - a hardware monitoring device that will check the power load generated by a power supply unit and give you an accurate reading of voltage being sent on each DC line.



**Soak Test**--it is common to let a test take place over a long period of time and to look for any changes or anomalies in the results. Typically, high-end graphics cards are soak tested before they are put into production to check that the card can handle large amounts of data and therefore high power consumption over a long period of time without causing excessive heat or damage to the card components.

Software Power monitoring tools are available to determine power usage by the server and other neighbouring devices. As an example the Dell PowerEdge contains its own monitoring software. Dell servers contain power supplies fitted with the PMBus specification - a 2-wire communications link providing power information to the monitoring software. Typical metrics include metrics such as voltage measurement and current level, component temperature, fan speed. Once gathered this information can be used by the system to intelligently throttle or to load-balance server clusters, ensuring that a server is not overworked.





# Loopback plugs

Loopback is both a command-line tool accessible through `IPCONFIG`, but also a low-level hardware plug capable of proving connectivity for a NIC port.





# POST card/USB

For more precise location you can use a USB or PCI POST card that has a digital output display providing a code number. This, when referenced in the manual will tell you precisely which component is not working.





# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Troubleshooting Common Hardware Problems:** <http://www.professormesser.com/free-a-plus-training/220-901/troubleshooting-common-hardware-problems-2/>
- **Hardware Troubleshooting Tools:** <http://www.professormesser.com/free-a-plus-training/220-901/hardware-troubleshooting-tools-2/>





## **901.4.2 Given a scenario, troubleshoot hard drives and RAID arrays with appropriate tools**

In the main, once set up correctly hard drives tend not to give too much trouble. However, there are various management tiers to consider - the physical drive(s), the RAID controller cards and their drivers, partitions, formatting types, disk management (basic or dynamic), the version of RAID / Storage Pool used, and finally the volume and its visibility.

In this section, we consider low-level and high-level issues that you will encounter and how to remedy them.



# Common symptoms

We are going to start by looking at low-level physical problems often caused by the fact that the disk is incorrectly seated, or worn with age. We will then look at the files used to identify partitions on the disk and where boot sectors can be found. We will then look at bootstrap files, issues specific to RAID and external pen drives. We end this section by looking at the built-in error-checking each disk can perform on itself.



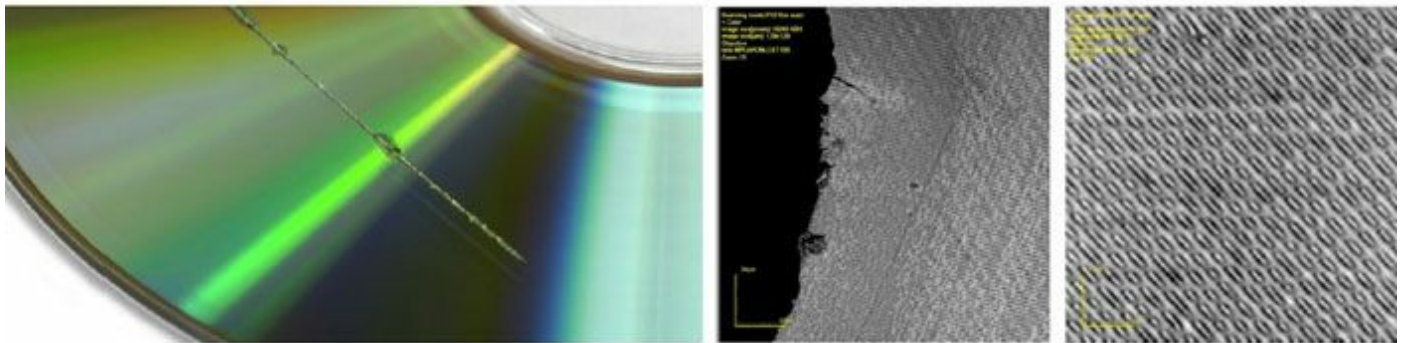
# Read/write failure

A system is in reality a variety of hardware devices working at different speeds having to agree common speeds. Self-checking mechanisms and communications protocols can check the integrity of the data in-transit, but there are times where, for example, mechanical failure can cause the data to be written incorrectly, or not at all. For RAM, dynamics memory requires a constant flow and recharging of power every few seconds to keep the data in RAM intact. Dynamic RAM is poor at retaining data and so data has to be constantly rewritten to.

There may be other reasons why it is not possible to write a file to a hard drive, for example, the user account instigating the command does not have the permissions to write to the drive, or you are trying to write to a DVD-ROM, but no DVD has been inserted in the drive, or has been physically removed mid-write operation.

I commonly had problems when trying to burn a CD on my older system due to the speed at which I was burning at caused the burn process to become unstable, or for the cache to fill up to a point where the burn process aborted, leaving a part-complete and unreadable CD (as the CD writing had not been finished and the ending section added to the burn).

Equally, reading an audio CD can be problematic if the media is scratched, causing parts of the CD to be unreadable. The PC will try to read the damaged section several times and at several different speeds, but often just cannot retrieve the data due to the physical damage.





# Slow performance

Hard drive performance can drop if the way in which we are writing to the partition has changed. Partitions are formatted into blocks (block sizes of 512,1024,2048 are common) and the amount of blocks in the partition is often managed by the OS and the best fit is found.

For file copying block-wise copying using iSCSI / FC or SCSI is preferable to SMB, which has to retrieve the file into memory first and then rewrite to the destination disk.

Of course, the speed of the hard drive has something to do with this as does the amount to which the volume is fragmented. To remedy these consider faster media (for example, SSD drives) or defragment the volume.





# Loud clicking noise

This is a horrible sound to hear as you are effectively witnessing the death toll of your hard drive. While it can be caused by an unseated hard drive and you may just need to check that it is screwed into place in the media bay and that the drive is level, it usually signals the fact that there is a physical, mechanical problem with the platters. A grinding or clicking noise is caused by the actuator arm actually touching the surface of the platter and you can bet that it is damaging it in the process. The actuator head is an electromagnet and hovers over the surface of the platter without coming into contact.

Should you hear this you are advised to swap the damaged drive for a known good or new drive immediately.



# Failure to boot

Boot problems are often caused by a number of reasons:

On a PC with multiple hard disks and multiple OS installed, the boot order in the BIOS is pointing the system to load the wrong hard disk. On this disk there is an MBR / GUID store that points the system to where the **Boot Configuration Database (BCD)** is stored. The OS marked as active is loaded at this point. However, if the bootstrap files are damaged or some missing, or the OS was not intended to be run on this system (for example, the disk was originally used on another significantly different PC with different specifications) the OS will be unable to boot.



# OS not found

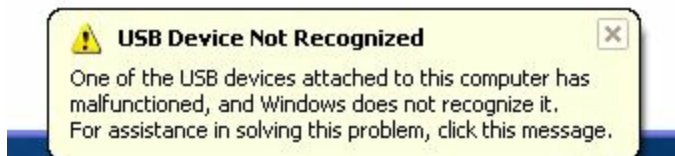
Assuming that the correct disk, MBR, and BCD were loaded the bootstrap files are missing in the location the system was pointed to. However, the message here will state that the OS was not found.



# Drive not recognized

Common with external USB drives (error 43) this message is not seen during the boot process, rather once the OS has loaded. It is common where a USB devices drivers have not been loaded. When you install a pen drive, for example, drivers are installed to govern the management of the hardware but also and importantly tie the driver to the specific USB port you have used. If you then plug the pen drive into another USB port the installation process will restart and the OS will think that this is a second USB drive. The same driver is used. The OS now has a dilemma - do I replace the existing driver? Has the first USB device moved or is this a new second device? Remember that some of this information is stored in the user's session.

Where this driver is incorrectly configured you will receive this error in the taskbar. One option you have is to upgrade the existing driver, or to remove and reinstall the existing driver. Ultimately, the cure is to restart the system and represent the USB drive once the OS is at contention. This problem was common with early XP machines, but is less common now with later systems as device management has matured.



This is why when you add a USB printer, but use a different port to the one you originally used the OS sets up the printer as a new printer and you see multiple instances of the same printer in the Devices and Printers window.



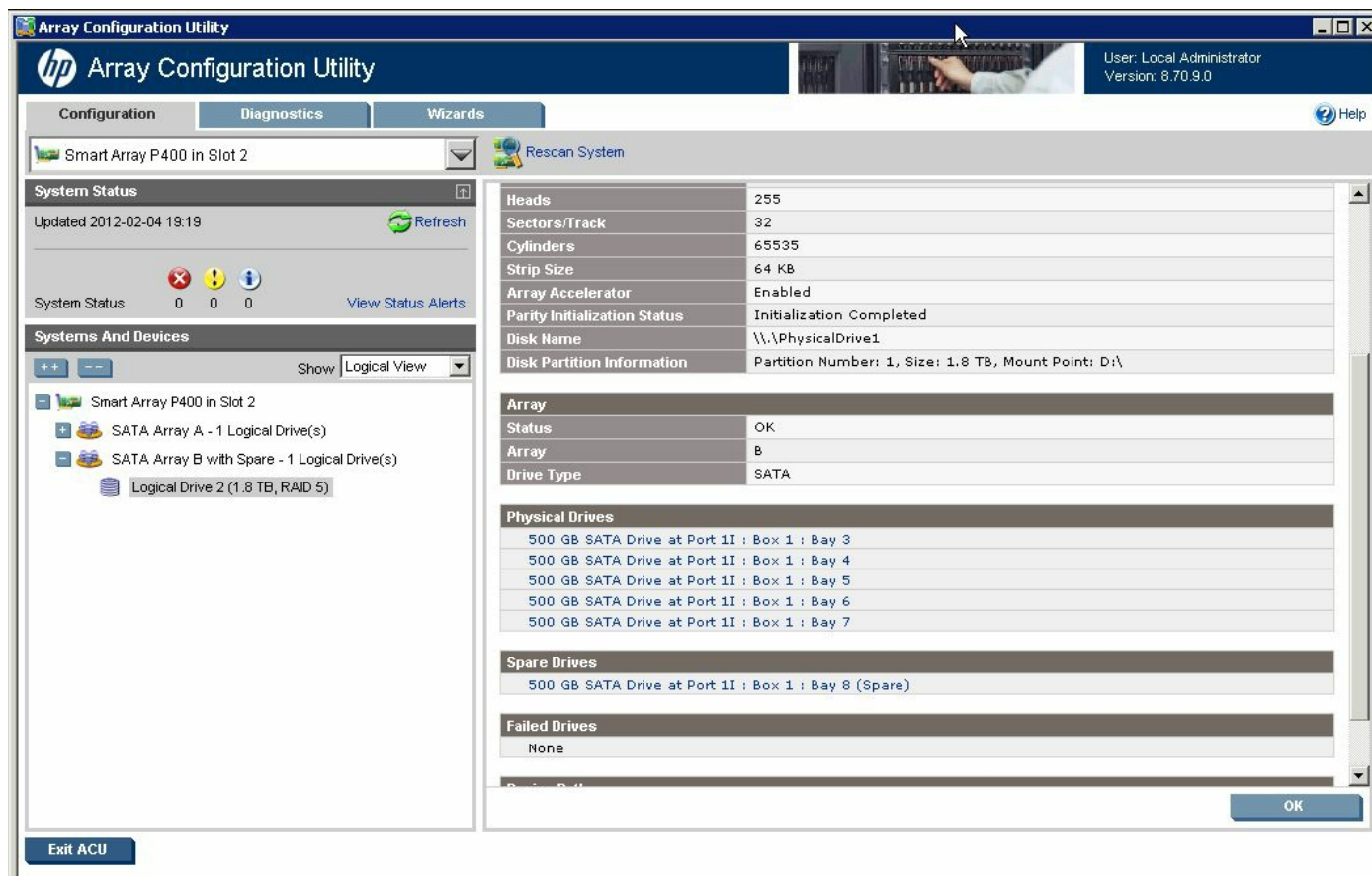


# RAID not found

The RAID array can either be managed by an independent hard disk controller and third-party software (Hard RAID), or by the OS. Where it is managed by the OS the Disk Management tool is used to group disks together to form a RAID array.

Note that Disk Management may show that the disks involved in the RAID group are not under the control of the OS, or may show that the disks are blank. This is because some RAID providers do not report back their RAID information to the OS and should be managed with their own third-party software.

RAID should never be used for the OS data itself, rather it is used to provide fault tolerance or read/write performance benefits for accessing your corporate data.





# RAID stops working

As RAID arrays are often independent of the OS it is possible for the RAID array to be disabled using the third-party program. This will make it stop working for all users on the network. If a Hard Drive has been ejected from an RAID 0 array, as all disks are needed for the volume to be accessible the entire volume will stop working. Reloading the disk may not immediately solve the problem as the volume will be marked as being in a problem state. To fix this the volume needs to be rescanned to make sure that all of the data is present by checking every stripe. This process of regenerating a volume can take up to several hours.

For this reason the RAID is kept on a server and therefore only users in the Active Directory Server Operators group can manipulate the RAID array.



# Proprietary crash screens (BSOD/pin wheel)

When the OS reaches a point where it becomes unstable, a monitoring module will freeze the OS and write critical information of the failure to the system event log so that the problem can be diagnosed at a later date. The user is shown a text display message with a copy of the information written to the log. This is irritating but helpful in that the error information can be researched and a problem diagnosed. Most often problems are caused because an app or another module within the OS has tried to write data into an active, reserved portion of memory already in use by the OS for something else, which is providing a critical underlying service.

The Apple pinwheel is irritating because you get no information about the error. You see the animation of a spinning pinwheel, indicating that the system is busy, whereas in fact the system has stalled.

This crash screen is known colloquially as the Blue Screen of Death, or the Spinning Pinwheel of Death.

For Windows systems ticking the automatically restart box described in an earlier section will negate the BSOD - the system will restart. An entry to the log will still be written, but this speeds up the recovery process. As a network administrator you need to decide if you want your end users to see these BSOD/SPOD messages.



# S.M.A.R.T. errors

Hard drives are now built and have been since 2004 with the Self-Monitoring, Analysis, and Reporting Technology built into the firmware on the disk controller card, located on the base of the disk drive. This is effectively similar to the POST test in that it can warn you of a suspect imminent failure in the integrity of the drive. There are however a number of problems with SMART:

You only know that there is a problem with this disk (that is, it is potentially damaged) when it already is or is acting out of tolerance settings:

- You cannot see any meaningful feedback - you get a text message during boot-up
- The operating system is not able to show SMART data in a meaningful way (you have to install a third-party app to make sense of the data)
- Manufacturers are not consistent in their handling of SMART

For the A+ we need to know that if you see a hard disk SMART error it is best to avoid using this disk.

Possible SMART apps you might like to consider are: HD Tune (<http://www.hdtune.com>) or Crystal Disk Info by Crystal Mark (<http://crystalmark.info/software/CrystalDiskInfo/index-e.html>)







# Tools

This section is going to focus on the software command-line (mainly) tools used to manage the disk, a partition and a volume. We will start with basic physical tools used to house the disk, but the assumption is that we are doing more than describing the insertion of an internal disk, rather setting up a series of disks as hot-swappable drives, built into a rack enclosure.



# Screwdriver

A screwdriver is a metal device with a pointed tip and a handle giving comfort grip and also the ability to apply rotational torque onto a screw. It is used to build the system and hold the various components in place.

Be careful never to attempt repairs without powering down the system, disconnecting it from the mains, and removing it to a workbench. Ensure that it and you are properly grounded with Electrostatic Discharge equipment such as a grounding mat, plug, and wristband before attempting repairs.

The trick is to never over-tighten the screw. Tighten until it gives resistance to further movement - this proves that the screw is completely seated in the screw hole (bore) up to the screw head.

Screwdrivers come in several types and it is common for a technician to have a variety of sized posi (also referred to as Phillips as this manufacturer used posi screws on their equipment), flat, and star headed screwdrivers.

You will often find in a screwdriver kit a pot to store the screws you have removed. This is useful.



# External enclosures

The system can expand physically outside of the PC chassis. Where equipment resides outside of the chassis it is said to be external (to the chassis) and needs to be connected by cabling conveying power and data. Some enclosures have their own power systems and data can be conveyed over the common standard existing data cabling such as Ethernet or Fiber cables and existing switches (for example, NAS and SAN).

Normally, when we refer to an external enclosure we are talking about space in an **Intermediate Distribution Frame (IDF)** for a tape backup drive / jukebox and hard disks that are powered and are either being used by the system as part of an existing volume / disk array, or are hot spares.





# CHKDSK

The disk checking tool (CHKDSK) is a common software command-line tool that checks the integrity of the hard drive by checking to see if a block of data can be written to and read from. Each block on the disk is checked along with the integrity of the volume. Where the fix parameter is applied, any errors are corrected (where possible) or the data is moved to a known good block and the damaged block is marked as bad.

Bad blocks are extremely rare and normally are caused through integrity problems linked to the volume format you have used, or the block sizes. Switching to ReFS or NTFS rather than FAT volumes will certainly help with this if you are sure that the problem was caused by the OS and not physical damage to the disk. If the disk is physically damaged it should be replaced immediately.



```
Administrator: Command Prompt

C:\Windows\system32>chkdsk
The type of the file system is NTFS.
Volume label is Win8_1.

WARNING! F parameter not specified.
Running CHKDSK in read-only mode.

Stage 1: Examining basic file system structure ...

    299520 file records processed.
File verification completed.

    4591 large file records processed.

    0 bad file records processed.
Stage 2: Examining file name linkage ...

    408190 index entries processed.
Index verification completed.

    0 unindexed files scanned.

    0 unindexed files recovered.
Stage 3: Examining security descriptors ...
Security descriptor verification completed.

    54336 data files processed.
CHKDSK is verifying Usn Journal...

    544034744 USN bytes processed.
Usn Journal verification completed.
Windows has scanned the file system and found no problems.
No further action is required.

62161919 KB total disk space.
53210124 KB in 234019 files.
150404 KB in 54337 indexes.
    0 KB in bad sectors.
902335 KB in use by the system.
65536 KB occupied by the log file.
7899056 KB available on disk.

    4096 bytes in each allocation unit.
15540479 total allocation units on disk.
1974764 allocation units available on disk.
```







# FORMAT

Before a volume can be used it has to be formatted. This process creates a block structure within the defined physical area of the drive that will be used by the new volume. A spiders-web of blocks maps out the surface area of the platters. Each block is identified positionally so that the OS knows where the blocks are.

**File Allocation Table (FAT)** is the oldest but most universal formatting structure. This supports a 32-bit block structure. FAT-16 was used by early Microsoft systems, but was phased out with Windows 95. FAT-12 was used for floppy disks and is unreliable. This too has been phased out. FAT volumes cannot have security permissions applied to them and to their folders, neither to compression or encryption hence the need for third-party compression and encryption tools such as 7-zip or WinRAR.

The **New Technologies File System (NTFS)** is now the common standard for all OS systems. (Apple can now support NTFS although a driver needs to be loaded first. Apple's default is exFAT). It has much better control of the integrity of the volume. It can auto-repair blocks and has a far greater performance benefit in comparison to FAT. It uses indexes to determine which blocks contain segments of a file. Additionally it can support and is the common standard for compression, encryption, and file security.

The **Resilient File System (ReFS)** is a new standard used on file servers where the integrity of the data needs to be assured. It is even better than NTFS in self-repair and supports extremely large volumes. The largest file that can be stored using ReFS is 16 exabytes and a volume size of 1 YottaByte.

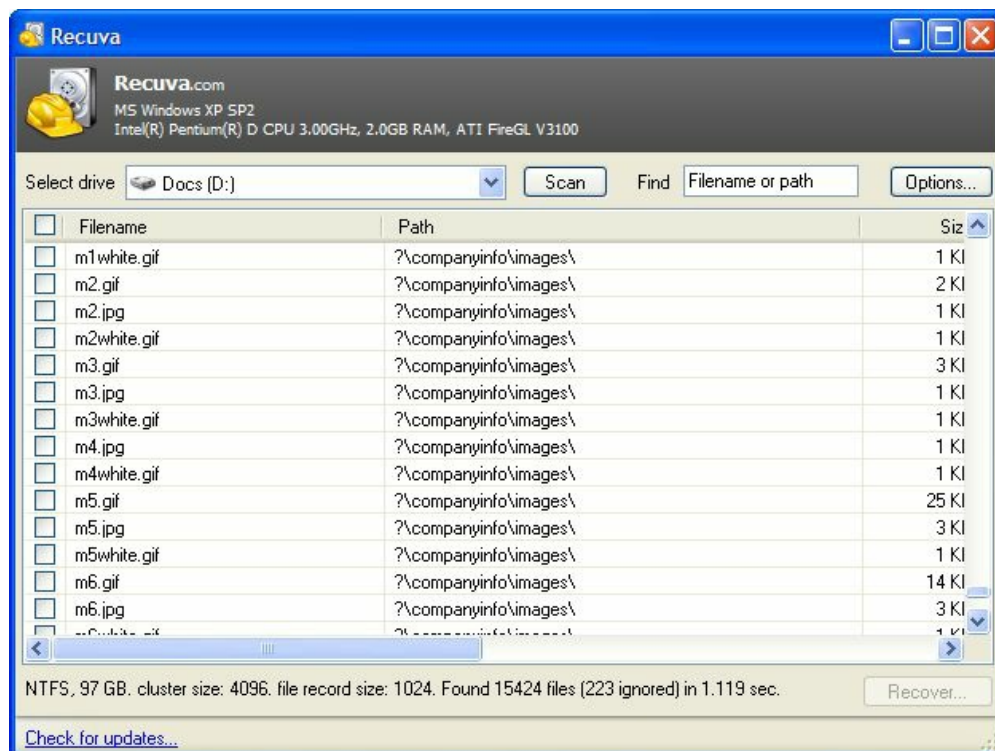


# File recovery software

If we assume that portions of the volume have not been written to or wiped, then the data is still there, electromagnetically and therefore can be recovered. When an end user presses delete and then wipes the file from the recycle bin, what has actually happened is that the first character in the filename that defines the file on the disk is cleared and the space used across the blocks is now available for the OS to overwrite to with new data.

Whist third-party software such as Piriform's Recuva is available Microsoft Enterprise partners have access to the Diagnostic and Recovery Toolkit - a downloadable suite of programs that can be saved to a bootable DVD-ROM disc (a public equivalent is the distro Hiren's Boot CD found at <http://www.hirensbootcd.org>).

All of these programs are a suite of low-level file recovery tools that allow you to be able to mark the start of a file on disk and for the program to then find all of the pieces of the file located across several blocks.





# Bootrec

Windows contains as a Recovery Environment - by accessing the advanced startup options you can instead load a command shell with a series of emergency tools to repair the system (you can also get to this prompt via the repair option if you boot from the installation DVD-ROM). `BOOTREC` (Boot Recovery) has a number of properties to fix different aspects of the boot process:

- `/Fixboot`: A new boot sector is written to the system partition. This option is best to be used where the boot sector has been replaced with a Vista or Windows 7 boot sector and by so doing your OS is inaccessible. If the boot sector was damaged, or if a legacy boot sector was written overwriting the more modern OS systems then you will not be able to load these. `/Fixboot` will perform a scan and find all compatible OS systems installed on the drive and re-add them in to a clean boot sector.
- `/ScanOS`: It will scan for OS systems (Vista and higher) and add these to the BCD store if there is not an entry for them already. This is useful if you have a dual-boot OS, but have moved the OS files, or edited the BCD manually and by so doing are pointing to the wrong volume, or folder location.
- `/RebuildBCD`: This is similar to `ScanOS`, but it completely rebuilds the BCD store, whereas `ScanOS` adds to the existing values.

The `BOOTREC` command can also be used with the Bootmgr is missing boot error message. Here, you can export the old BCD store and then rebuild the BCD store from the exported file.





# DiskPart

DiskPart is a very powerful tool allowing you to perform drive and volume changes (for example, to extend and shrink a drive, create a new volume, and assign a volume letter) just as in the Disk Management graphical tool. DiskPart can also be used to define a partition as the active partition and by so doing assist the system to find the MBR/GUID table and from here to locate the volume containing the BCD. It is a command tool similar to `NSLOOKUP` or `TELNET` in that once invoked the command window changes to the DiskPart environment. To close your session and return to normal Command Prompt you type `EXIT`. DiskPart uses common, easy to use commands:

- `ACTIVE`: Lists the chosen partition as the active partition.
- `LIST/ADD DISK`: Lists the disks on the system. Add Disk is used when setting up a disk mirror to add the second disk to the set (Windows 7 and higher).
- `ASSIGN`: Used to assign a mount point or drive letter to the chosen disk.
- `ATTRIBUTES`: Shows and sets the security attributes for the current selected volume.
- `AUTOMOUNT`: Allows Windows to mount and assign a drive letter to new disks.
- `BREAK DISK`: Used to break a disk mirror.
- `CLEAN`: Wipes the disk entirely. `CLEAN ALL` also sets every bit on the entire disk to 0 (a low-level format).
- `CONVERT`: Used to convert a basic disk to a dynamic disk and vice versa. It can also be used to convert an MBR boot record to GPT and vice versa.
- `CREATE`: Used to create a new partition, or volume.
- `DELETE`: Used to remove a disk from the list of disks. It does not wipe the actual disk. With partition it does remove the partition references from the MBR/GPT. With volume you can delete a specific volume from the disk.
- `DETAIL`: Provides details of the disk / volume / partitions available to the system.
- `EXTEND`: Used to extend a partition
- `LIST`: Used to show the volumes / disks / partitions for the user to select and to work on.
- `SELECT`: As list. This sets `DISKPART` to focus on the specific object you have asked for.
- `SHRINK`: As `EXTEND`. Used to shrink a partition.

This is not an exhaustive list, but it covers most main functions.



# Defragmentation tool

Over time files become fragmented. The reason for this has to do with how SMB writes to the disk. The system looks for the next block with available space and tries to write the file to that space, but does not think ahead. As the file is saved it is split into small sections with parts of the file spread across several blocks. Where possible the system will prioritize the process of filling the blocks to make best use of the available space. Usually the files are written to contiguously (so after block 1000 is full the system moves onto 1001 if it has space free, and so on.). Sometimes there is a jump as the neighboring blocks already have data stored there, so it then finds the next available block, and so on until all of the file has been saved.

This leads to a messy situation where files are split up and stored in multiple block locations. This is referred to as fragmentation. Anything over 5% is considered a problem as the process of reading and writing files to and from the disk gets ever slower and the system has to work harder.

To overcome this a defragmentation tool undoes this by collecting all of the pieces for the file and saving them contiguously where there is enough space. The file is therefore easier for the system to retrieve.

For mechanical disks fragmentation is a problem and a regular Defrag after maintenance (for example, uninstalling a program) is advised. SSD drives do not require defragmentation as the access time to get data is the same from any of the memory locations across the SSD disk (which in reality is a group of silicon chips, not a mechanical drive).



Windows 8, 8.1 and 10 perform automatic maintenance tasks including defragmentation. If you are using SSDs please configure this to not defragment your disk otherwise it will shorten the life of the SSD drive.

Each system has its own Defrag tool already built in so there is really no need to buy or use a third-party tool, however, there are a lot of these available on the market and these give a nice disk display, showing a visual representation of the state of the disk.

Piriform Defraggler

Action
Settings
Help

Drive	Media Type	Capacity	Used	Free Space	Fragmentation	Status
Local Disk (C:)	SSD (NTFS)	128.3 GB	66.2 GB (52%)	62.1 GB (48%)	Unknown	Verify Complete
Data (D:)	SSD (NTFS)	110.1 GB	92.7 GB (84%)	17.4 GB (16%)	76%	Analysis Complete
Archive (E:)	HDD (NTFS)	465.8 GB	391.2 GB (84%)	74.5 GB (16%)	19%	Analysis Complete
Seagate F...	HDD (NTFS)	465.6 GB	288.9 GB (62%)	176.7 GB (38%)	Unknown	Analysis Aborted

Analyze Drive

Defrag Drive

Quick Defrag Drive

Advanced

Drive E:

File list

Search

Drive map

Health

Status

Analysis Complete

Disk Health: **GOOD**

Analysis results:

35 Fragmented Files (77.9 GB)

125 Total Fragments

19% Fragmentation

View files...

Benchmark drive

Properties

Used space:

420,075,409,408 bytes

391.2 GB

Free space:

80,029,278,208 bytes

74.5 GB

Capacity:

500,104,687,616 bytes

465.8 GB

Analyze

Defrag

Pause

Stop

[Online Help](#)
[Check for updates...](#)



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Troubleshooting Hard Drives:** <http://www.professormesser.com/free-a-plus-training/220-901/troubleshooting-hard-drives-2/>
- **Hard Drive Troubleshooting Tools:** <http://www.professormesser.com/free-a-plus-training/220-901/hard-drive-troubleshooting-tools-2/>
- **Troubleshooting the Boot Process:** <http://www.professormesser.com/free-a-plus-training/220-901/troubleshooting-the-boot-process/>



## **901.4.3 Given a scenario, troubleshoot common video, projector, and display issues**

Although the main portion of this section is going to focus on symptoms and how to correct them we are going to use this opportunity to talk more broadly about video display and some of the additional considerations you might have, especially concerning the display output (Hue, Brightness, Gamma, artifacts) and the physical projection of the display (for example, Keystoning and Skewing).





# Common symptoms

There are a number of reasons why you will see no output but they amount to a few common problems:

- There is no power to the monitor
- The video data cable is either not connected or the input selector on the monitor is set to a different port that is currently not being used
- The resolution broadcast by the PC is not one which the monitor is capable of presenting, so either gives out the best it can (a garbled image), or a blank screen
- The output data signal is too weak (sometimes the case with DVI connections and long cables), or of the wrong type (DVI-I can send either Digital or Analogue signals, but the monitor may only be able to use one type)
- The driver is corrupted, or not working as expected, so either an alternative driver needs to be installed, or the driver needs to be rolled back to a known good that will require first putting the PC into basic VGA mode



# VGA mode

VGA mode (640 x 480 dpi) is a basic resolution standard for all modern PCs and monitors. If you have selected that the graphics card display a resolution that is not supported by the monitor, the screen output will become garbled and impossible to read. To help with this Windows gives you a number of seconds to answer a question - do you want to keep this new setting or revert back to the previous one?

It is very easy to not read the message, or ignore it, or to click keep without thinking about what you are doing and then to close down the PC at which point your settings are saved.

Not entirely. As long as you do not log in on the sign-in screen (assuming the resolution has not at this point changed to the new settings) then your previous settings are saved in the older version of your profile. The moment you do sign in this known good is wiped and lost, replaced by your misconfigured new profile. As a result the OS doesn't know that there is a problem, but you can't see the screen.

So the first point of call is the advanced startup setting last known good configuration that basically uses the previous version of your profile when you do log in, taking things back a step, as it were.

If Last Known Good is not an option to you, Enabling VGA mode will load the system in the lower resolution, returning you to a viewable desktop. From here you can set the screen resolution to what it should be.



# No image on screen

We are here assuming that this is an output data problem and not a cabling or power problem.

There are several reasons for no image on the screen - where you have a second monitor, check that you are projecting your output profile to both monitors (there are two settings for projecting to two monitors - extend the desktop, or duplicate screen 1). If this does not apply to you, that is, you only have one monitor; check the input selector on the monitor itself is looking at the correct cable (most monitors support different cables, so they have different options for composite, component, HDMI, DVI, and SVGA).



# Overheat shutdown

If you are using a projector you will notice that it will get hotter over time. Projectors have a tolerance, but if the heat builds up within the projector bypasses the tolerance level the device will enter a cool down state and if still not corrected will force a shutdown. This is commonly caused by dust and other particles obstructing the flow of air into the unit and it may be the case that the input air intake filters may need to be changed.





# Dead pixels

Over time certain pixels cannot be energized - this is usually due to a hardware fault and not something you can fix. It is best to check the device at different resolutions. If you are watching a movie and it only occurs when that specific movie is played the fault may be with the recorded movie itself and not with the monitor.



# Artifacts

More common with CRT monitors, if the refresh rate is low a ghost image can remain on the screen for some time as the phosphor glow dissipates. This remnant image is known as an artifact.



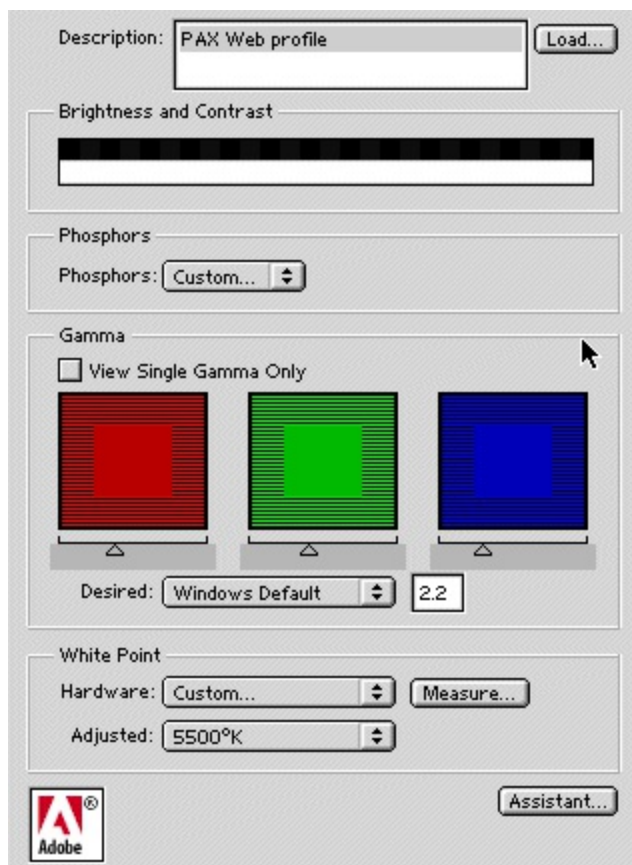
# Color patterns incorrect

Each monitor takes the video data and interprets it in slightly different ways. The monitor itself is manufactured with different tolerances and if you compare like-for-like several manufacturer's monitors you will notice differences in the gamma, hue, brightness, and contrast - the same image will not appear exactly the same on all monitors.

This is a great cause of concern for graphic designers and video editors who need the image they are working on to be the same, consistent, across all monitors.

When working with digital camera images the file format RAW is used which as well as keeping the data in an unaltered state also supplies the calibration data from the camera. This is also different with every digital camera.

For this reason manufacturers provide color profiles and monitor drivers for the OS to use to know what the tolerances and differences are from a common standard.









# Dim image

A dim image is typically caused by a low brightness, or Gamma setting, causing the image to be displayed darkly. There are separate system settings and monitor settings. It is best to reset the monitor settings and to adjust the settings to taste from within the OS.



# Flickering image

The refresh rate is measured in Hertz (cycles per second). The screen will refresh typically 50 or 60 times per second. For gaming this can be much higher with 120 Hz quite common.

If the monitor does not support the refresh rate you have selected one of two things might happen--the image will be drawn off-center and smaller/larger than expected, or a flickering will be observed.

The refresh rate should match the supported rates for your monitor. Typically a standard monitor supports 60 Hz. This can be set in Desktop | Screen resolution | advanced settings | Monitor tab.



# Distorted image

The most common cause of a distorted image, assuming that there is nothing wrong with the saved image itself and in fact the entire screen is being affected, not just the area where an image is being displayed, is that the resolution has been set to a non-standard type that is not supported by the monitor. The monitor is overlapping pixels to try its best to display at the selected resolution, but this creates a soft image.

The default native resolution always provides the most crisp display and is the system setting you should aim to keep unless you have a good reason not to use it.



# Distorted geometry

With CRT monitors in particular you can move the width and height of a picture, but also the starting x and y axis positions. By doing so, the footprint image being displayed on the screen can be moved to the correct position. If these settings are incorrect the image will be skewed and part of the image may not display.

On projectors it is also common to be able to skew the image by using either keystoneing or trapezoiding the image. This setting is used on fix-mounted (ceiling or desk mounted) projectors who are projecting at a viewing angle that is not direct at the screen. With ceiling-mounted projectors for example, keystoneing can adjust the relative width between the top lines and the bottom lines that compensates for the fact that the projector's position is causing the image to splay onto the screen.



Without Keystone  
Correction



With Keystone  
Correction





# Burn-in

Similar to ghosting, if you leave a monitor presenting the same image for a long period of time the screen will be energized at those pixels for far longer than they need to be causing damage to the pixels at the positions where the image was being displayed. When the monitor is turned off it will be possible to see a faint shadow of where the light areas in the image was.

You can protect from this by using one of two features:

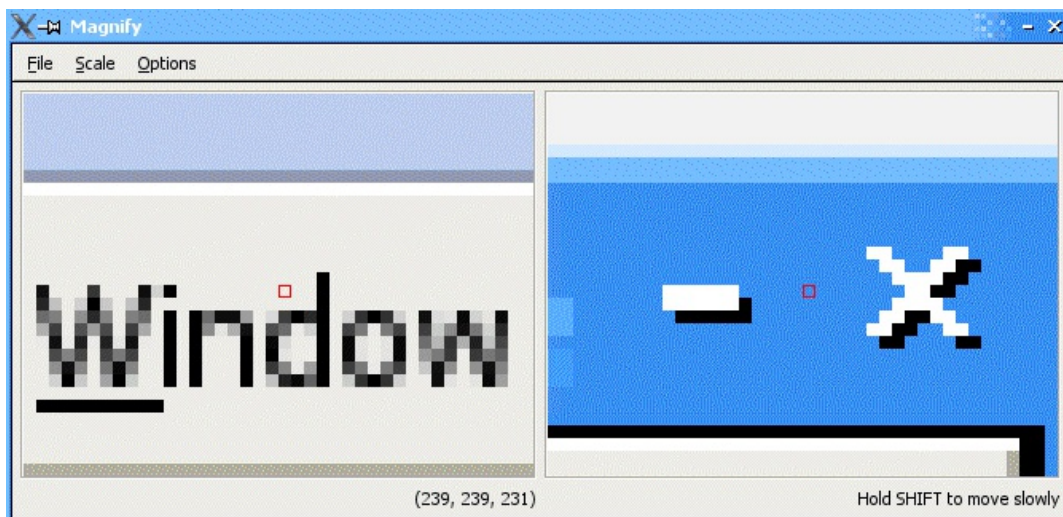
- **Screensaver:** By setting a screensaver the image will constantly change, causing no one area to be over-energized
- **Power options:** By turning the screen off after a few minutes of inactivity you can stop this from occurring



# Oversized images and icons

There are several ways in which the image can be oversized:

- The user has turned on a Zoom / magnifier tool, or visual impairment tool to magnify parts of the screen. Turning this app off will return the display to normal settings
- The user has selected a large icon size format on the theme
- The user has selected a lower resolution. The footprint will be smaller, but the icons will appear larger





# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide.

- **Troubleshooting Video and Display Issues:** <http://www.professormesser.com/free-a-plus-training/220-901/troubleshooting-video-and-display-issues-2/>



# **901.4.4 Given a scenario, troubleshoot wired and wireless networks with appropriate tools**

This is a very interesting and I hope you will also find it to be a useful section as here we are going to look at an assortment of key scenarios that you will regularly and repeatedly encounter. For some of this, with you management hat on, you will be able to plan ahead and put together safeguards and measures to prevent these from happening again, but for the moment we are going to concentrate on the symptoms and their fixes, focusing on wired and wireless network connectivity.





# Common symptoms

We're going to approach this from the aspect of the various problems you will encounter. We will describe the problem and look at a series of fixes that will remediate the problem. As always with this, refer to the OSI model to help to guide you through your problem-solving, pinpointing the exact nature of the problem and assisting you in your fix.



# No connectivity

In terms of the OSI model, when used as a troubleshooting guide I often start at layer 1 (physical layer) and work my way up from there to determine at which point within the network design my problem is occurring. If you are using a wired connection such as Ethernet, you will get a status light on the NIC itself, at both ends of the cable, so on the PC NIC and on the Switch port. This proves an electrical connection is made between the two devices.

The connectivity light, however, does not prove that the TCP/IP stack is in use, or any other communications protocol is working correctly.

Within the Network Connections page you will see a not connected status against your NIC if physical connectivity is the problem.

For Wireless NICs, moving the laptop to another location and connecting onto a different network, then returning to your original network does not necessarily mean that your Wireless NIC will automatically connect to your access point. For this you need to trigger the Wireless Networks pane (in Windows 8 or higher) and press the Connect button.

When using a VPN, the same is true - you have to manually press the Connect button in order to establish the connection.

## Networks

Airplane mode

Off



### Connections



da.installers.dk  
Connected



Installers VPN



sstp.solrod.dk



vpnadmin.cloudapp.net

### Wi-Fi

On



DRG-3204  
Connected



Hessellund



RedhatFiber



# APIPA/link local address

Originally designed as Network Zero back on Windows 2000 systems, this was Microsoft's attempt to automatically generate IP addresses for PCs on the same subnet - you need never worry about IP addressing ever again, or so we thought.

**Automatic Private IP Addressing (APIPA)** is now used as a fall back system and is common on all Windows PCs where the IP address is automatically assigned from a DHCP server. The leased client IP address is typically available for eight days and this number is part of the known private classful addressing system (for example, the range 192.168.0.0-255 for class C networks) and these are routable--a router can perform **Network Address Translation (NAT)** and allow the private device to access the internet.

The problem is that APIPA addresses are not routable. When the DHCP server is not available and a heartbeat signal generated by the server cannot be found, over time the client PCs will fall back to use instead APIPA addresses. All APIPA addresses start 169.254.x.x where x.x is a series of numbers from the range 0.0 to 255.255. Each PC takes a random number from this range and therefore are on the same subnet (169.254.0.0) so it can communicate with each other, but not outside of the network. This makes APIPA good for local working (for example, Workgroups), but a serious problem for Domain Networks where internal routers will not pass APIPA traffic out of the subnet.

If you know that the DHCP server is working and can access the domain from other computers in the same subnet then your problem PC may simply need to request to return to use its leased address. By performing an `IPCONFIG /RENEW` the DORA process is triggered. As the MAC address of your client PC is known you should get back the same IP address originally assigned to your PC. With this the PC switches back to using its assigned classful private IP address.



# Limited connectivity

Connectivity is considered to be limited when restricted to send traffic only within the subnet. In this situation you would ping the router using its internal IP address first (the one on your subnet), then an exterior IP address (for example, one in the other subnet the router services). If this second ping is successful then it proves that your internal router is not the problem.

Next we try the edge router--this is the gateway to the internet and by pinging its Public IP address we are testing connectivity.

Internet Service Providers lease public addresses for a limited time and these can change often. Usually this makes no difference to the edge router and it is this router that will track and manage the IP address change.

So connectivity is limited when the external network is not accessible. Here you would again use logic to stretch out from your PC with PING tests advancing to the edge of your network, then beyond to external resources. I find that `PATHPING` or `NSLOOKUP` of [www.google.com](http://www.google.com) or Google's public server: `8.8.8.8` a good test.



```

C:\WINDOWS\system32>nslookup 8.8.8.8
Server: SkyRouter.Home
Address: 192.168.0.1

Name: google-public-dns-a.google.com
Address: 8.8.8.8

C:\WINDOWS\system32>pathping 8.8.8.8

Tracing route to google-public-dns-a.google.com [8.8.8.8]
over a maximum of 30 hops:
  0 MBITT1.Home [192.168.0.43]
  1 SkyRouter.Home [192.168.0.1]
  2 * * *
Computing statistics for 25 seconds...

```

Hop	RTT	Source to Here Lost/Sent = Pct	This Node/Link Lost/Sent = Pct	Address
0				MBITT1.Home [192.168.0.43]
1	2ms	0/ 100 = 0%	0/ 100 = 0%	SkyRouter.Home [192.168.0.1]

```

Trace complete.

C:\WINDOWS\system32>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=19ms TTL=60
Reply from 8.8.8.8: bytes=32 time=15ms TTL=60
Reply from 8.8.8.8: bytes=32 time=17ms TTL=60
Reply from 8.8.8.8: bytes=32 time=23ms TTL=60

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 23ms, Average = 18ms

```



# Local connectivity

Local connectivity, as in the preceding section refers to the fact that only local resources can be contacted. This is the case where external-facing routers, or ISP connections are not working. Where the internal router neighboring your PC is not working you are restricted further to resources within your subnet only.



# Intermittent connectivity

There are occasions where other equipment may conflict with your connectivity. This is common with crosstalk on wireless devices - the same channel and 802.11 protocol is being used by two physically adjacent devices. When the second device is active, it can generate a signal that interferes with the signal from your PC, causing your connectivity to drop out.



# IP conflict

Each IP address on the subnet needs to be unique. If two devices are using the same IP address and one of the PCs has its IP address assigned via DHCP, then the DHCP-enabled PC will reset to 0.0.0.0 (meaning I am not on any network) until the problem is resolved. It is possible that the other system with a manually-set IP address has had its number set in error, as it is conflicting with a DHCP scope - that is a range of IP addresses given out by a DHCP server. However, if the manually-assigned IP address is correct the DHCP scope can be altered on the server to omit the offending IP address from the range (this is referred to as an exclusion). This is often done for servers or early network-enabled photocopiers where the IP address had to be hard coded into the device's firmware.





# Slow transfer speeds

As part of the TCP/IP handshake, the two devices agree speeds that can be used to send data. The data stream starts with the slowest speed and is then sped up to faster speeds up to a fastest the other PC can handle. If the PC is hard-coded with settings defining a slow speed then it can only transmit at this slow speed.

For example, if I am using an 802.11g router but connecting with a 802.11b wireless card, as G is backwards-compatible with B both will transmit at the slower speed.



# Low RF signal

The strength of the wireless signal is measured by a series of five bars, or as a percentage. If the signal strength is over three bars (55% or higher) the signal is said to be acceptable and the session can continue. The weakness of the signal means that it is harder to hear and likely that the signal will be prone to interference, or crosstalk meaning that the amount of errored packets will increase. This will slow down transmission as packets will need to be resent. When the signal drops below tolerance (different on every device but usually around 50%) the session may break and connectivity drops.



# SSID not found

One of the security measures I would recommend is that when you have set up all Wi-Fi devices on your network to turn off the ability to broadcast the SSID, on your router / Wi-Fi access point. The SSID is the station identifier - a name by which the access point is known and this is used to establish which access point of several in the vicinity you are connecting to, when you create a Wi-Fi profile on your PC.

Once the profile is made, you already know the name of the access point, but there is no benefit in broadcasting this name to the public. With a smartphone a nosey person, or legitimate hacker could walk past the access point, perform a Wi-Fi scan, and get a list of all available access points in the area. There is nothing wrong in this, but do you want a complete stranger connecting to your router? Why even broadcast that you have a router in the area?

The SSID not found message is usually seen when you are creating a Wi-Fi connection profile on your PC, but have spelt the name of the SSID wrong. Turn the router's SSID back on temporarily, check the spelling of the name and then once you are set up, turn the SSID back off.



# Hardware tools

You will regularly refer to and use an array of hardware tools, used to check functionality, or to create customized cables for plenum runs or patch cables connecting from the Patch Panel to the Switch on each **Intermediate Distribution frame (IDF)**. You will also need patch cables (straight-through cables) to connect the PC to the wall socket. However, your cables must be wired correctly and be able to take the signal along the maximum distance allowed by the media, shielding from interference or cross-talk. For this you need to check your handiwork, such as with a Cable Certifier to ensure that the cable is not only fit for purpose but meets building regulations (where the cable is 'in-situ').

This section will look at an array of network cable and other hardware tools essential to the IT technician.

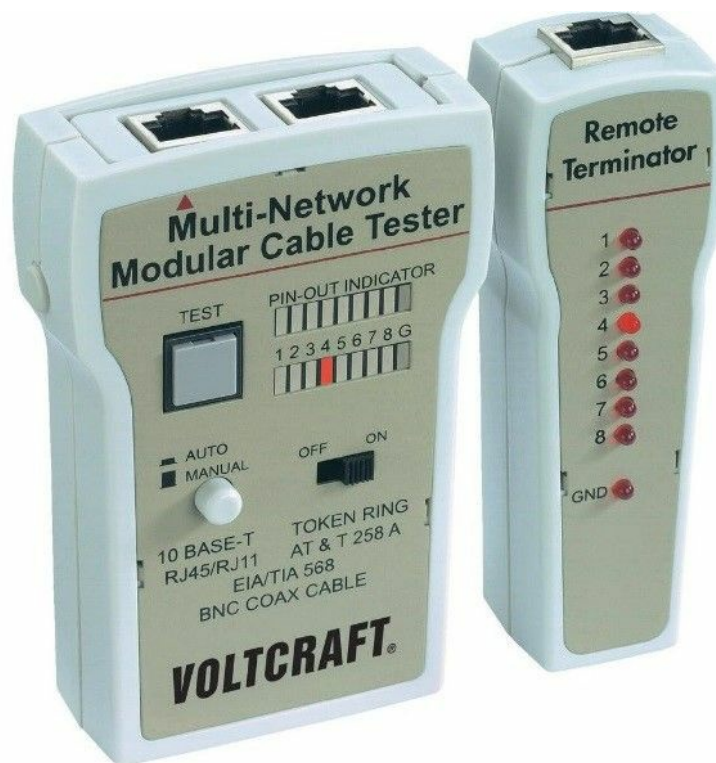




# Cable tester

A cable tester is a device that will check for electrical continuity in a network cable. One end of the cable is connected to one end of the device, the other end is connected to the other side of the device. A test electrical signal is sent on each wire in turn, lighting LEDs on both sides of the device. Any break in continuity either by socket pins not connecting to the cable it is crimped to, or a wire break within the cable itself will cause the LED pair not to light up.

A cable tester is often used to ensure connectivity on manually-crimped cable during the cabling of patch and installed cabling (for example, the void area in a false office ceiling, also known as Plenum space).





# Loopback plug

Loopback is both a command-line tool accessible through `IPCONFIG`, but also a low-level hardware plug capable of proving connectivity for an NIC port.





# Punch-down tools

A punch-down tool is a pen-like device with a v-shaped metallic end. It is designed to apply pressure onto a wire, forcing it in the v-slit of the 110-block. The same tool is also used on telephony headers such as are at the reverse of RJ45 network points, or ISDN sockets, although screw-held equivalents are also still possible to buy.

As the force is applied to the wire, the punch-down tool allows downward force to push the wire into the slit. As the slit narrows the plastic jacket is cut and the wire is exposed, making tight contact to the V-slit, also holding the wire into position.





# Tone generator and probe

Imagine a scenario where you need to label patch cables in a switch room, but the patch panel has been left as a mess and you need to determine which end is for which cable. To find the end of a cable can be difficult. A Tone probe can help here. This is a device in two parts - a sounder and power unit to send a signal across the cable and a screwdriver-like a sensor that is tapped on the end of the cable until the correct one powered by the probe's power unit is found at which point a beep is sounded. A common make is Fox and Hound and this is why the toner probe is still today referred to as that. Electricians also use single-unit toner probes to determine where live wires are housed within walls to ensure that they do not inadvertently drill into a power cable.





# Wire strippers

Wire strippers are a nutcracker-like device screwed at the very end with a series of pre-cut holes where it is possible to apply pressure to and cut into the plastic sheathing around a wire and therefore allow the external plastic sheathing to be severed so that it can be manually pulled away from the wire and removed by the operator. Different size diameter holes are present to enable the operator to strip different types of wire, from power-rated wires to small telecoms thinnet or telephone cabling.



# Crimper

Cable crimpers are a multi-purpose device used to strip, align and cut the cable and internal wires, but also to attach the RJ45 pin-outs to their respective wires. A Crimper blade is first used to cut the cable to length, the jacket is then carefully cut revealing a length of wire, which is untwisted, straightened, and put into the correct positioning. The wires themselves are then dressed (placed against each other) and the wire tops are again cut to ensure equal length. The wires are then passed into the RJ45 plug and pushed to the very end where they lie behind the copper pins, within their respective 8 wire channels. The crimper is then used to apply pressure onto the copper pins that bite into the wire ends, making contact with the copper below the plastic sheathing. At the same time a bridge component is pushed down onto the cable jacket at the base of the plug, tightening a grip over the wires and cable, holding the array into place.



To make your own Ethernet cable, you'll want:- A length of unused cat 5e cable up to 100 meters (usually 2 or 5 meters is fine).- A crimp tool- x2 RJ45 boots (rubber jackets)- x2 RJ45 sockets



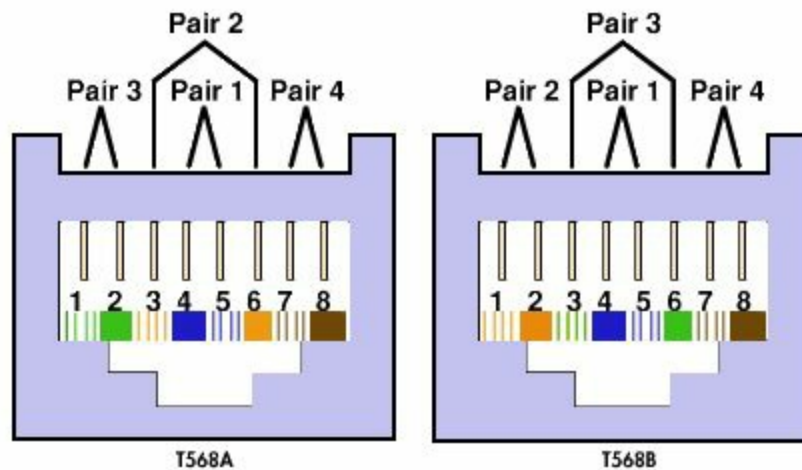
NB: You can purchase two different types of socket. One has the top and bottom sections as two plastic pieces that lock together when crimped. This is easier to place the wires into their respective channels than the second full socket type where you have to push the wires into their respective lanes and may jump track when threading the wires in.

Using the stripping razor on the crimp tool, strip 3-5 millimeters off the sheath at the end of the cable. Be careful not to shear the internal wires. Also remove the plastic cladding

and any shielding foil. Untwist the ends of the wires and place them between your finger and thumb with the wires in the correct order for TIA-568A or B, depending on which schematic you are following. Pinch and level out any kinks in the wires so that they are absolutely straight. Use the blade if need be to ensure that all of the ends are completely level.



NB: If you are planning to make a Straight-Through (Patch) cable then the wiring must be same at both ends of the cable. For a Crossover cable swap wires 1 with 3 and 2 with 6.



Place the boots onto the cord, to be fitted to the sockets later on.

Place one end's wires into the socket ensuring that all wires are in their respective channels and are at the very end of the channel so that when crimped will make good contact with the pin underneath it.

Place the socket into the crimping tool and tighten. This will lower the pins, cutting through the plastic sheath and making contact. Secondly, the base of the socket has a plastic clip that will lower onto the outer plastic of the cable, holding the socket into position. Please ensure that the clip bites into the casing and not onto the exposed wires.

Repeat this for the other end.

Fit the boots around the base of the socket. This will give the cable more durability.

Connect both ends to a cable tester and check for connectivity on all eight wires.





# Wireless locator

The process of scanning for wireless networks within immediate range without the permission of the person transmitting with an intent to connect to one of these wireless networks is referred to as War Driving. Network analysis software can be relatively basic (such as Wireless Zero Configuration), which will display local wireless networks.

Another useful tool is Wi-Fi Planner for Aerohive Apps (available at <http://www.aerohive.com/planner/>) that can provide a 2D map of the building and overlay a 'heat map' of wireless transmissions. This can assist with determining where to place access points to ensure for the widest coverage.

A wireless analyzer is an application containing a suite of the preceding features, providing network analysis, scanning, and problem detection. It is common that a wireless analyzer will contain `ping` and `SNMP` command systems so that once a picture of local transmitters has been determined the user will be able to send test packets, or to test the integrity and security of the packets, whether they have an SSID broadcast as part of the packet or not. It used to be the case (in previous Network+ versions) that one way of increasing the security of a network would be to disable the SSID as then the packet would be transmitted but would be invisible to the client. Although this is true more sophisticated applications such as wireless analyzers, or even dedicated wireless analysis probes will still be able to read the transmitted packet and perform a packet sniff. An example phone app providing these features is Network Analyzer Lite, available on the iTunes store (<https://itunes.apple.com/gb/app/network-analyzer-lite-wifi-info-scanner-ping/id562315041?mt=8>).





# Command-line tools

We're now going to focus our attention at some of the command-line tools used regularly to resolve network issues. Working your way up the OSI model, I would advise that the approach you should take is as follows:

Do I have a working NIC? Is it enabled? Test this by checking Network Connections. Does it report back with a Network name, unknown network, or unplugged? Using the CLI, PING Loopback. This proves that the NIC is working by sending a test packet within the NIC.

Now that I know the NIC is working do I have an IP address? Try `IPCONFIG` to determine the IP address. Make sure that this is in the same subnet and also that you have an entry for the gateway (router). Also check that your subnet mask is the same as other PCs on the subnet. You can even try to `PING` another PC on the subnet.

Now, `PING` the Router's internal IP address. If successful, `PING` the external IP address. This proves the Routing table is correct. Next, `PING` a known PC on the other subnet. Lastly, `PING` an Internet address (for example, `PING 8.8.8.8`, which is Google's DNS server).

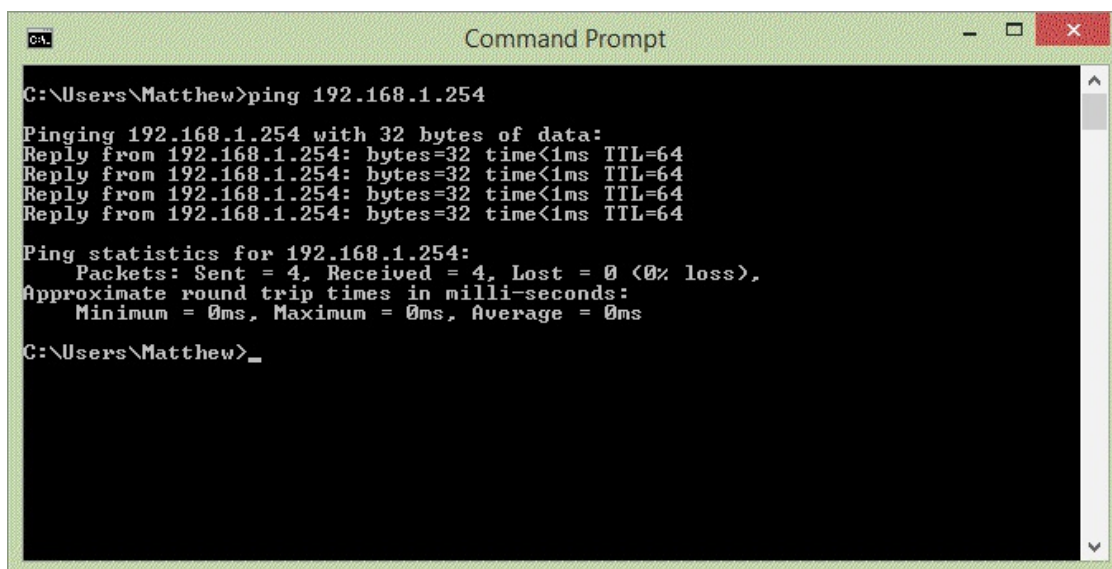
If the issue is in resolving names to IP addresses, make sure that you have an entry for your DNS Server's IP address within your NIC profile. `PING` the DNS server, then `PING` a computer elsewhere on the network you have not contacted yet, proving that a DNS-fetch is occurring.



# PING

**Packet Internet Groper (PING)** is a major tool in the ICMP suite. However, routers and managed switches can block ICMP traffic. PINGs are a major cause of **Denial of Service (DOS)** as a PING command can be looped, or can be sent indefinitely (known as the Ping of Death). A ping is a test packet sent to a specific IP address. Domain names can also be pinged and the test packet is resolved and sent to the machine we are trying to reach. A ping command sends four test packets of a set size, in sequence and records the time taken for a response to be received. This enables us to see if the next node in the network map from this point can be reached and also if there is any congestion on the cable, or if the node we are trying to reach is itself congested.

By pinging a node several hops away in a physical sequence (for example, through a switch, through a router into another subnet, through a switch and then to the end node) we can determine if this path is viable. This will suggest to us if there is a break in the path (for example,, a disconnected cable or a misconfigured router).



```
C:\Users\Matthew>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Matthew>_
```

On an IPv6 network, the Ping -6 switch will send an IPv4 test packet. In the case of the following example I am Pinging the loopback address for IPv6 on my local NIC. By doing this we are proving that the NIC is working, that the TCP/IP protocol stack is working, that IPv6 is enabled and that the NIC is able to process this data.



NB: Ping6 was a separate command to perform this action on XP systems.

```
Command Prompt

C:\Users\Matthew>ping -6 ::1

Pinging ::1 with 32 bytes of data:
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms

Ping statistics for ::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Matthew>
```

In the preceding screenshot, what we are however not testing is the physical condition of the actual port within the NIC. To do this, we need to use a loopback plug that will send any outward bound data back in through the input pins creating a data loop and affirming connectivity.

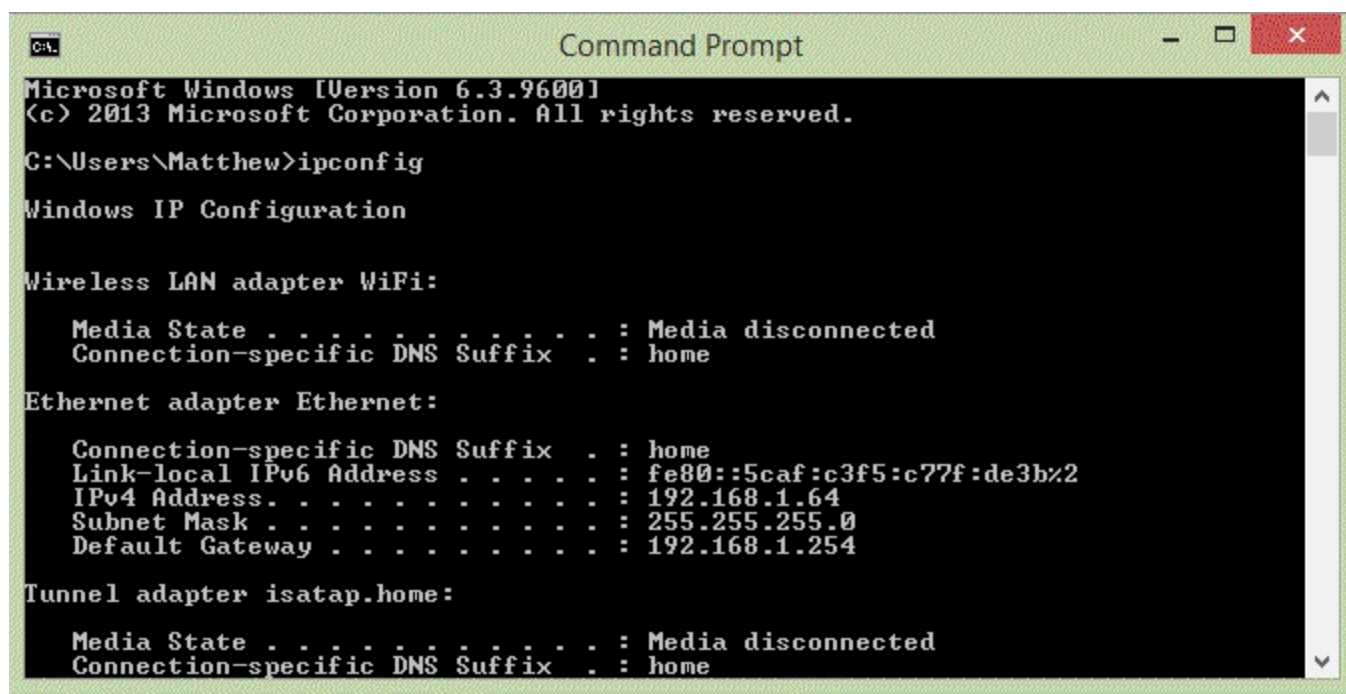




# IPCONFIG/IFCONFIG

IPCONFIG (IFCONFIG on Linux systems) is a command-line tool that provides basic IP configuration data for all NICs and Tunnels on the system. Using the default command with no switches will give the main IP address for the system, however, `IPCONFIG / ALL` is useful in that it also provides additional information such as:

- Whether the host IP address was provided by DHCP
- The media state (for example, Wi-Fi may be disconnected)
- The host NIC IP address, subnet mask, and default gateway
- The MAC (link-local) address of the NIC



```
Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Matthew>ipconfig

Windows IP Configuration

Wireless LAN adapter WiFi:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : home

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . : home
    Link-local IPv6 Address . . . . . : fe80::5caf:c3f5:c77f:de3b%2
    IPv4 Address. . . . . : 192.168.1.64
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254

Tunnel adapter isatap.home:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : home
```

Additionally, with the `/ALL` switch we can learn:

- Hostname and DNS information
- IP address of the `DHCP` and `DNS` servers
- `DHCP` lease expiry
- Are we using NetBIOS over TCP/IP

This tool makes for a good starting point to determine the IP configuration settings of the host NIC quickly. If there is a misconfigured gateway, that may be the reason why a NIC can communicate with other systems in the subnet only.

An IP address statically assigned to the same IP number as another system will cause a conflict on the network. If the IP address is assigned by `DHCP` what should happen is that the configurable IP address (DHCP) will default to `0.0.0.0`, meaning cannot communicate to any host on any network, prompting you to set an IP, or to check for IP conflicts. This can be a common problem for legacy photocopiers and printers that had to be manually assigned an IP address in the firmware.

The `IPCONFIG` tool also can be used to flush the DNS cache of any rogue entries. If the system has been the victim of DNS poisoning, the `/FLUSHDNS` switch will clear the local DNS cache and prompt the client system to check with the DNS server for any new requests.



Exam Tip: Expect to be asked about an APIPA scenario, where the DHCP server is uncontactable either due to a BOOTP router blocking traffic between subnets, or a DHCP server is turned off. APIPA is an emergency system (used to be referred to as 'Network zero', or 'auto configuration') whereby all hosts on the subnet obtain an IP address starting `169.254.x.x` where `x.x` is a random set of numbers. The idea is that each IP address should be unique. However, APIPA addresses are non-routable, so it is not possible to use a host in an APIPA state for internet connectivity.

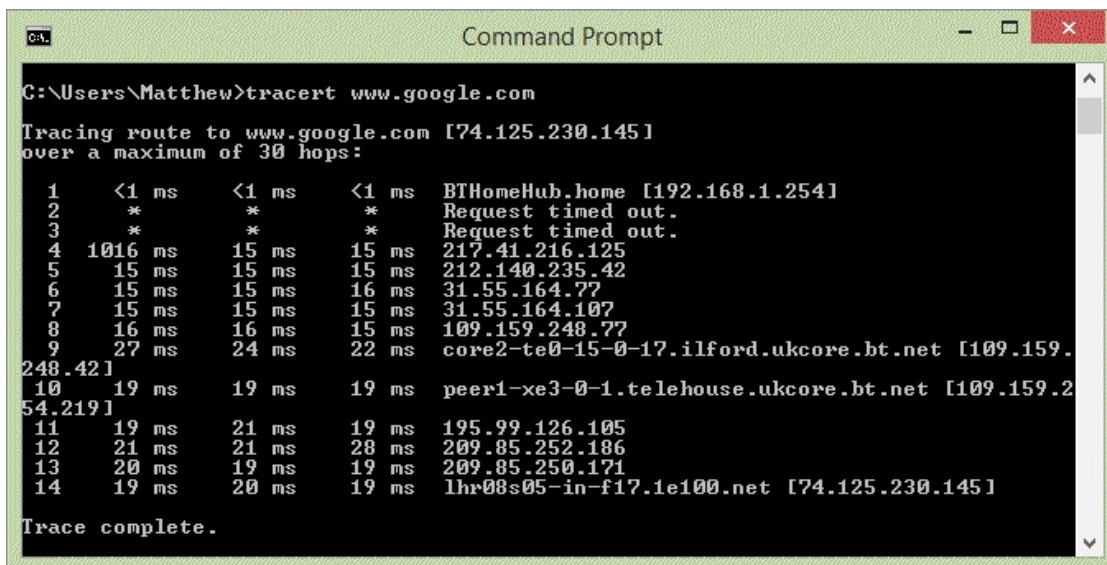




# TRACERT

Traceroute (Tracert on Microsoft Systems) is a command-line tool that will show the path taken to send data packets across the network. For the internal network it will show common pathways or trunk lines used to reach the destination. The use of the -6 switch (or on some systems 6 is appended to the command name) infers that the trace will take place using a test IPv6 packet.

Traceroute is useful as a mapping tool to determine the pathways taken from router to router to ensure that no routing loops are occurring, or to check that the most effective route is being chosen. If the Network manage is aware of a faster route at one point in the pathway, they may choose to amend the router configuration to favor the preferred route.



```
C:\Users\Matthew>tracert www.google.com

Tracing route to www.google.com [74.125.230.145]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    BTHomeHub.home [192.168.1.254]
  2  *         *         *         Request timed out.
  3  *         *         *         Request timed out.
  4  1016 ms   15 ms    15 ms    217.41.216.125
  5  15 ms     15 ms    15 ms    212.140.235.42
  6  15 ms     15 ms    16 ms    31.55.164.77
  7  15 ms     15 ms    15 ms    31.55.164.107
  8  16 ms     16 ms    15 ms    109.159.248.77
  9  27 ms     24 ms    22 ms    core2-te0-15-0-17.ilford.ukcore.bt.net [109.159.
248.42]
10  19 ms     19 ms    19 ms    peer1-xe3-0-1.telehouse.ukcore.bt.net [109.159.2
54.219]
11  19 ms     21 ms    19 ms    195.99.126.105
12  21 ms     21 ms    28 ms    209.85.252.186
13  20 ms     19 ms    19 ms    209.85.250.171
14  19 ms     20 ms    19 ms    lhr08s05-in-f17.1e100.net [74.125.230.145]

Trace complete.
```



# NETSTAT

NETSTAT is a command-line tool showing all currently active connections on the system. This is useful to determine if there are any unknown background services attempting to communicate without the knowledge of the user.



```
C:\Users\Matthew>netstat

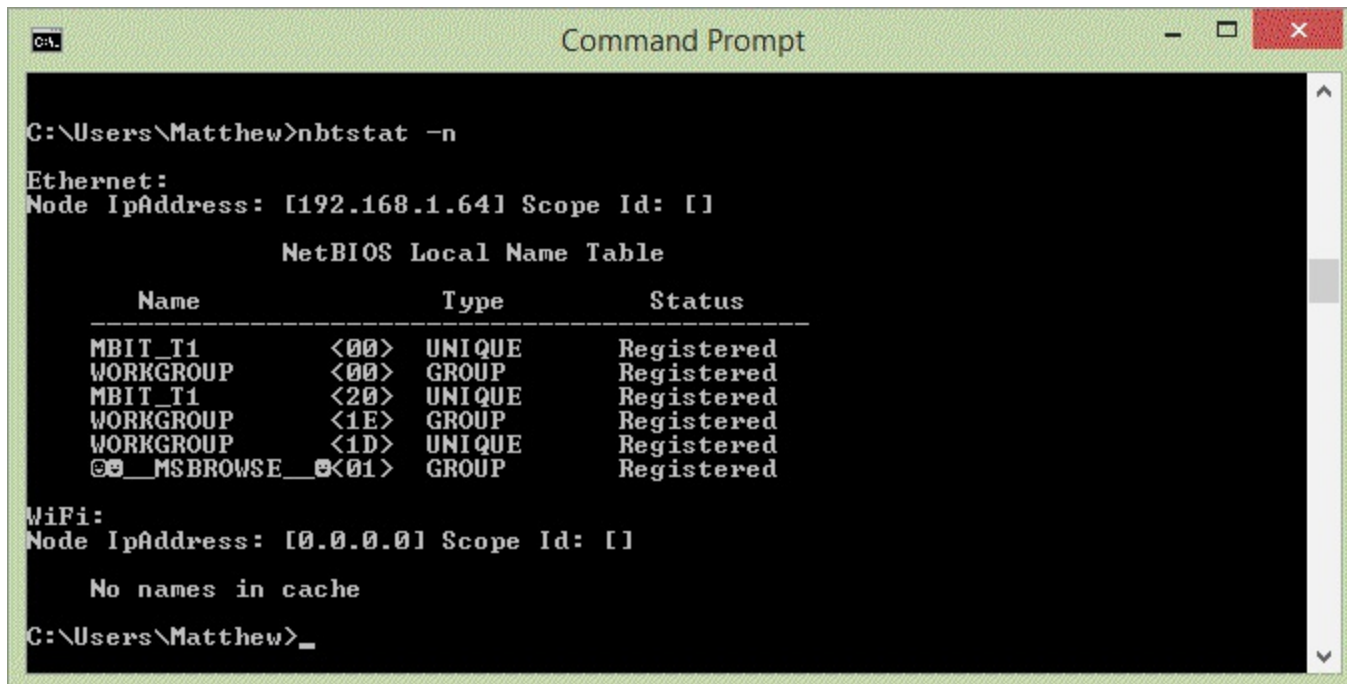
Active Connections

Proto Local Address          Foreign Address         State
TCP    192.168.1.64:49187      157.55.236.57:https     ESTABLISHED
TCP    192.168.1.64:49289      a23-35-218-254:https    CLOSE_WAIT
TCP    192.168.1.64:49325      ec2-23-21-169-76:https  ESTABLISHED
TCP    192.168.1.64:49326      lhr08s05-in-f24:https   ESTABLISHED
TCP    192.168.1.64:49327      lhr08s05-in-f4:http     ESTABLISHED
TCP    192.168.1.64:49328      lhr08s05-in-f23:https   ESTABLISHED
TCP    192.168.1.64:49329      lhr08s05-in-f3:https    ESTABLISHED
TCP    192.168.1.64:49330      lhr08s05-in-f24:http    ESTABLISHED
TCP    192.168.1.64:49331      104.28.17.108:http      CLOSE_WAIT
TCP    192.168.1.64:49332      104.28.17.108:http      ESTABLISHED
TCP    192.168.1.64:49333      lhr08s05-in-f26:http    ESTABLISHED
TCP    192.168.1.64:49334      lhr08s05-in-f26:http    ESTABLISHED
TCP    192.168.1.64:49335      108.162.202.131:https   ESTABLISHED
TCP    192.168.1.64:49336      108.162.202.131:https   CLOSE_WAIT
TCP    192.168.1.64:49338      lhr08s05-in-f23:http    ESTABLISHED
TCP    192.168.1.64:49339      lhr08s05-in-f5:http     ESTABLISHED
TCP    192.168.1.64:49340      lhr08s05-in-f5:http     ESTABLISHED
TCP    192.168.1.64:49341      lhr08s05-in-f13:http    ESTABLISHED
TCP    192.168.1.64:49342      lhr08s05-in-f13:http    ESTABLISHED
```



# NBTSTAT

NBTSTAT is a useful tool for displaying NetBIOS statistics on the internal network.



```
C:\Users\Matthew>nbtstat -n

Ethernet:
Node IpAddress: [192.168.1.64] Scope Id: []

        NetBIOS Local Name Table

    Name                Type               Status
    -----
    MBIT_T1              <00>    UNIQUE        Registered
    WORKGROUP            <00>    GROUP          Registered
    MBIT_T1              <20>    UNIQUE        Registered
    WORKGROUP            <1E>    GROUP          Registered
    WORKGROUP            <1D>    UNIQUE        Registered
    *MSBROWSE__          <01>    GROUP          Registered

WiFi:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

C:\Users\Matthew>
```

NETBIOS is a legacy system used in the days of Windows 95 and NT. It was a simplified version of DNS that was flat in structure, not hierarchical. The **Windows Internet Naming Server (WINS)** is an earlier, basic version of the modern DNS in that it resolved hostnames to IP addresses. NETBIOS protocols can be run across the TCP/IP network for backwards compatibility. With modern system it is unlikely that network problems will be presented if the corporate network has moved over to DNS. However, workgroups and home groups may be misconfigured, or may contain hidden groups in use by spyware. These may be revealed through the use of NBTSTAT.

There are several switches connected with NBTSTAT. Usually you will want to run the command to resolve names and to view remote tables from other neighboring hosts. Switch:

- -a will resolve a remote host by its name
- -A will resolve a remote host by its IP address
- -R will reload the NETBIOS cache
- -s lists the session table
- -RR releases and refreshes the NETBIOS system, clearing the cache and restarting communication with WINS





# NET

The **network (NET)** command is a highly used and popular way of performing most network tasks. It has been used for several decades on most PC systems, however, it is worth mentioning that Microsoft are planning to phase out the NET command and replace it with a series of PowerShell commandlets.

On Windows 8 and higher, if you are running a PowerShell session, but invoke the NET command you are in fact running PowerShell equivalent commands. Here, we are going to refer to the traditional use of NET as seen on a DOS Command Prompt.

Some of the things we can achieve with the NET command are to manage network shares, create, and delete network print jobs, add and edit network users. Only NET commands still valid with Windows 7 and higher are in the following list:

- **NET Accounts:** This is used to set the password, or change password or other user account settings.
- **NET Computer:** This is used to add or remove a computer from the domain.
- **NET Config:** This shows the key information about how the current device is set up, as a workstation, or as a server.
- **NET Continue:** NET can be used to pause background services. This command continues the paused service.
- **NET File:** This provides a list of all files currently open on the PC. If a file is locked (because it is in use) this command can remove the lock allowing the file to be deleted.
- **NET Group:** This is used to add, delete, or modify a global Active Directory Global group.
- **NET Help:** To find out where to start the Help command can provide specific information for each of the Net subset commands.
- **NET Helpmsg:** If you have encountered an error message you will notice that it has an error number. Either search the Microsoft online knowledgebase site, or use this command to get detailed information about the error.
- **NET Localgroup:** As with NET Group, but services local groups on the local SAM database, not Active Directory.
- **NET Pause:** Pauses a background service running on this computer.
- **NET Session:** This is used to connect or disconnect sessions to another PC on the network.
- **NET Share:** This is an extremely popular command. It creates, manages, removes a



shared folder on the network. The Share is also assigned to a Volume letter on the PC, so NET SHARE K: \\mynetwork\myresources would allow me access the MyResources folder on my file server as drive K.

- NET Start/Stop: These are used to start or stop a specific background service.
- NET Statistics: This is a connectivity report showing key network statistics for your PC.
- NET Time: This is used to show the current time of a PC. You can also view the time for other PCs, so if a PC has fallen out of scope because its time is 10 minutes different to the Domain Controller (for example, the Lithium BIOS battery is old and needs to be replaced, or the time has been manually altered) you will be able to check without needed to log in on the remote PC.
- NET Use: This command shows a list of all current shares on your PC.
- Net User: This is used to add, edit, or remove a user from the current PC.
- Net View: This provides a list of known PCs and other network devices, currently known to your PC.



# NETDOM

This powerful command-line tool allows a network administrator to manage Active Directory Domains and Trusts from the Command Prompt. This is the equivalent to the GUI Active Directory Domains and Trusts on Server 2012:

- With the `NETDOM` command you can:
- Join a client PC (XP or higher) to a domain
- Add, manage, or remove computer accounts from Active Directory
- Add a Computer account into an Organizational Unit
- Move a Computer account from one domain to another, where a trust is in place
- Establish a one or two-way trust relationship between two domains
- Reset the secure channel for a Computer account that is no longer trusted by AD
- Manage an existing trust relationship



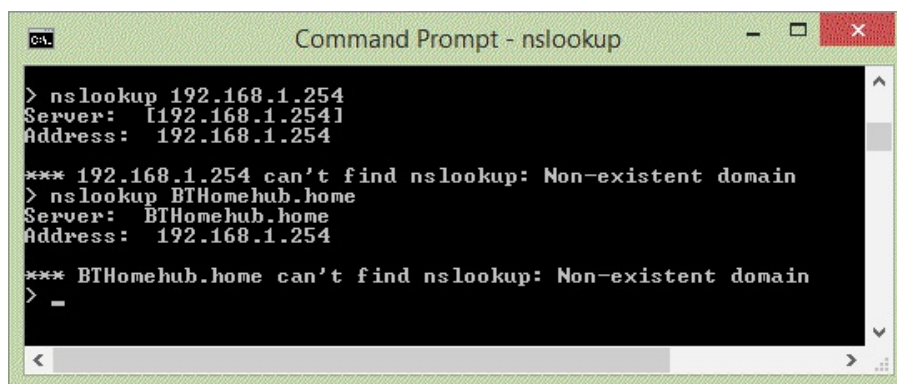
A full list of commands is available at: [https://technet.microsoft.com/en-us/library/cc772217\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc772217(v=ws.11).aspx)



# NSLOOKUP

**Name Server Lookup (NSLOOKUP)** is a command-line tool environment. It is a powerful tool able to print, but also to set domain information. It is used to edit the local NS cache. Typically, `NSLOOKUP` will list the location of the default local gateway by its DNS name and IP address, however, more extensive configuration of the local NS table can be performed. As modern domains rely on the presence of a DNS server `NSLOOKUP` is only used to edit specific configuration cache information, although it is often easier to flush the cache with `IPCONFIG`. `NSLOOKUP` is used to manually locate and to resolve other servers and routers across the network.

A DNS server can forward a request to another (parent) DNS server (for example, in a Branch Office connected to Head Office scenario. Here the branch DNS only has local entries - anything else needs to be forwarded on to the Head Office), or can forward its request to the internet. The **Internet Assigned Numbers Authority (IANA)** are responsible for managing root-level internet name databases (for example, `.com`, `.org`, `.uk`, and so on. The servers hosting these root zone databases are referred to as root hints) and report back the public IP address of the entry point into that company's network. If I run an `NSLookup` against [www.microsoftcoursesuk.com](http://www.microsoftcoursesuk.com), and my client computer has never been there the request is dealt with by my local DNS server. If there is no entry for it in its database, the result is forwarded.



```
Command Prompt - nslookup

> nslookup 192.168.1.254
Server: [192.168.1.254]
Address: 192.168.1.254

*** 192.168.1.254 can't find nslookup: Non-existent domain
> nslookup BTHomehub.home
Server: BTHomehub.home
Address: 192.168.1.254

*** BTHomehub.home can't find nslookup: Non-existent domain
> -
```



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Troubleshooting Networks:** <http://www.professormesser.com/free-a-plus-training/220-901/troubleshooting-networks-2/>
- **Network Troubleshooting Tools:** <http://www.professormesser.com/free-a-plus-training/220-901/network-troubleshooting-tools-3/>
- **Network Troubleshooting at the Command Line:** <http://www.professormesser.com/free-a-plus-training/220-901/network-troubleshooting-at-the-command-line-2/>





# **901.4.5 Given a scenario, troubleshoot and repair common mobile device issues while adhering to the appropriate procedures**

In this section, we will consider how to repair mobile devices such as smartphones and comment on some of the best practice guidelines and procedures to follow.



# Common symptoms

Most mobile devices are not user-serviceable. They will need specific, specialized parts from the manufacturer and the tiny screws are headed with non-standard points, so standard posi or flat screwdrivers (even watchmaker size) may not be able to help you to repair it. Nevertheless you will need to identify problems with the device and determine to what extent you can repair faults.



# No display

If there is no display at all when the device is powered we must first check that the device is actually powered. Most smartphones do not have a power LED, so replacement of the battery for a charged, known good would be the first thing to try.

If the display provides an EGA post screen or Samsung splash screen (for example), this is a good start as it proves the display itself is working as is the adapter.

Locked phones at this point also will provide an animation of the phone provider (for example, O2).

If these are displayed then the answer is likely to be with display settings within the OS. You can boot into an advanced startup menu on most phones by pressing the volume up, select and power keys at the same time, when powering the smartphone. Here you can select a safe mode option where any misconfigured display settings can be returned to normal.

Smartphones are not user-serviceable. A broken or cracked screen will not necessarily stop the display from working although parts of the display may not render. If this is the case the entire screen will need to be replaced.



# Dim display

The brightness settings on the phone can be easily accessed by swiping down the settings menu. At the lower part of this is a brightness slider. This should be set to 50% mid-way for everyday use. If set to a low setting the display may be unreadable.





# Flickering display

As with no display, a flickering display implies an intermittent fault with the power, or data flow to the screen caused by poor wiring or damage to the internal circuitry. This will need to be checked by an expert and is not user-serviceable.



# Sticking keys

Laptops or tablet-style devices will have a keyboard that is prone to damage. While the Surface may look cool, its keyboard is very thin and easily broken.

As with PC keyboards, laptops will suffer if liquid (for example, pop or coffee) is spilled over the keys. Whilst most of it can be wiped up and the keyboard face cleaned, some may seep into the crevice between the button and keyboard decal where it will dry on the lower portion of the button, causing it to stick. Denatured isopropyl alcohol can be used (with care) on the keys to remove any dried residue, however, this procedure can be extremely difficult on devices like the Surface where the keyboard cannot be taken apart.



# Intermittent wireless

When considering the cause for intermittent wireless connections consider the following:

- Distance from your router. Am I too far away to get a strong and stable signal?
- Is my router in a central location? Is my router placed next to a large device such as a refrigerator that may impede the signal?
- Is another device on the network sharing the same channel? What happens when I disconnect this other device?
- Am I also using a phone connection? Are all of my phone sockets in the building fitted with an ADSL micro-filter?
- If I change the channel of my wireless router, does this make a difference?



# Battery not charging

Laptop batteries on modern systems, especially HP laptops, also receive a special ID signal through the power cord, generated by the PSU. This proves to the device that a genuine PSU is fitted (HP laptops do not work from universal PSUs). If you try to boot from a non-standard PSU, even though it may be supplying the correct power settings (voltage and amperage), the absence of this signal means that the laptop battery will deliberately not be charged.

Some laptops, as a preventative measure stop charging the battery when the laptop is overheating. To test this switch off the laptop and attempt to charge it once the laptop is cold.





# Ghost cursor/pointer drift

The ghost cursor happens when an application is not correctly rendering the mouse cursor, but the laptop is still recognizing the moved coordinates from your mouse. Here, you would need to close the affected app and check that your cursor is viewable on the screen, then restart the app.

Accelerometers can be linked to the cursor, or even a laser mouse on an uneven surface, or glass table may cause inferred movement in the pointer. Usually, moving the mouse by hand resets the mouse to a specific position. In the case of the glass table, placing the mouse onto a dark surface, or mouse mat will solve the problem as the laser beam is no longer being deflected.



# No power

It sounds like the original IT joke: Have you turned it off and on again? (The IT Crowd), but in fact this is a fair point. Using the OSI model and starting with the physical layer are we getting power? If so, to what extent are we getting power? Is the monitor separately powered? Is the PC booting? Do we hear any change in the chassis - are fans whirring? Do keyboard lights turn on? Is there a Power LED present?

Modern PCs use a soft power facility meaning that there is residual power going to the motherboard at all times. This low-power is enough for the power monitor and soft switch to be supported that once triggered brings the power consumption up to full power usage and triggering the POST and Boot sequences.



# Num lock indicator lights

As part of the POST process, on a PC the USB /or PS/2 keyboard receives power immediately. This is proven by the Num Lock indicator light that is defaulted to be on. By toggling Num lock, Caps Lock, or Scroll Lock you should see the lights turn on and off once keyboard presses are being listened to by the system (after POST but before the bootstrap).

Most POST systems also flash all three indicator lights on the keyboard for one second to prove that all three buttons are working.



# No wireless connectivity

Wireless devices have an airplane mode setting which, when turned on, disables all forms of radio communication from the device. The idea was to allow users to continue to use the device whilst on an airplane, as any RF communication may interfere with the radio equipment used by the pilot. Therefore with airplane mode on all RF signals are stopped.





# No Bluetooth connectivity

Bluetooth is an additional drain on power, so needs to be turned on before you can use it. Next you need to discover the Bluetooth device you are connecting to, often protected by a 4-digit pin code. Once the connection has been established you will then be able to share to this device.



# Cannot display to external monitor

As with Bluetooth above the external monitor needs to be discovered and a connection established (for example, using Chromecast or similar feature). Remember that you need to undergo the process of discovering and connecting to the internet-enabled TV and also have device drivers installed compatible with the presentation system you are using.



# Touchscreen non-responsive

The screen might not be responsive if you have the smartphone inside of a plastic protection case that may impact on the working of the touchscreen. Then, clean the screen with a lint-free cloth to ensure that no oil or dirt could be impacting on this feature. If the screen does have oil or dirt on the screen only the oily part would have been affected.

If the whole screen is non-responsive consider a restart.



# Apps not loading

Apps usually do not load if the hardware does not meet the app's requirements, or supported underlying software such as a graphics driver is present, or has the capability needed for the app to load. An example may be a game requiring DirectX graphics acceleration, but the available video memory is low, or DirectX acceleration is not supported by your graphics card.

For laptop systems a more recent OS should be backwards compatible for most apps, but you always tend to find that a few just stubbornly will not load. We have a compatibility view option on the app shortcut to force the app to load using architecture and settings for a previous OS version. This usually solves the problem, but in severe cases you might need to consider either creating a Virtual Machine containing the previous OS, or dual-booting the laptop.





# Slow performance

Smartphones, as well as laptops become filled with junk temporary and cached files, over time which can reduce performance. Use programs such as **Ccleaner** to remove these additional files that are no longer needed.

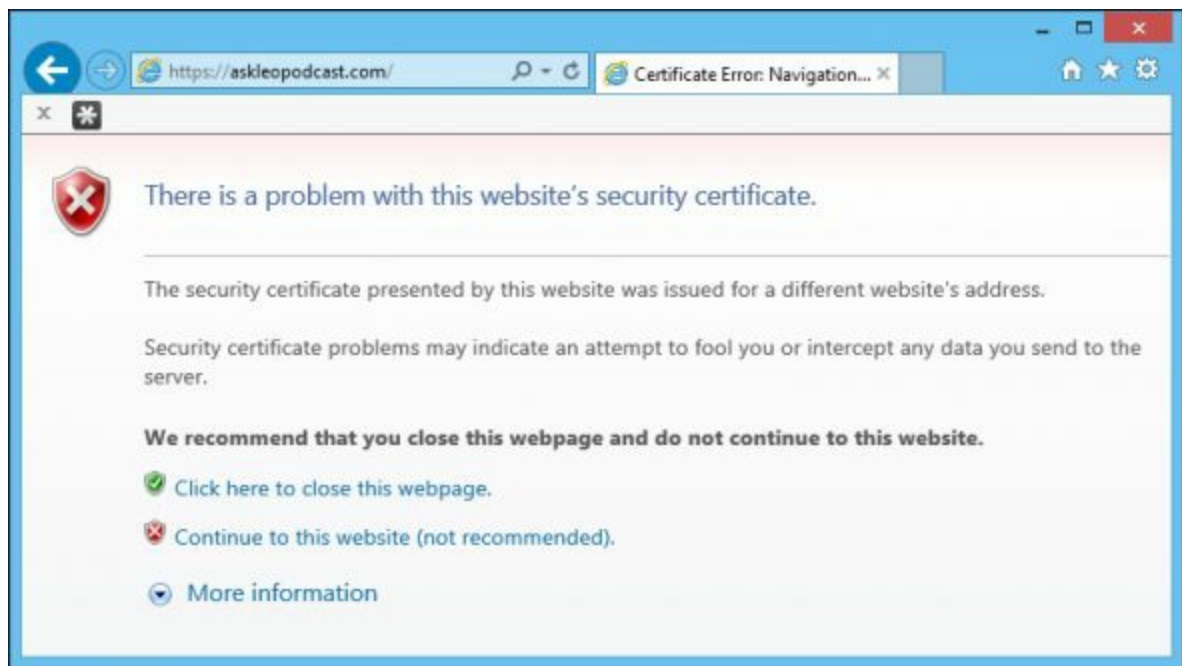
Running too many apps at the same time also causes a drain on the amount of additional RAM available for us to use. Manage your running apps and consider adjusting the startup settings so that only the essential apps load on startup, the rest you can trigger when you need to use them.



# Unable to decrypt email

On corporate networks email is sent to your client PC in an encrypted form. You should have received and installed a certificate from your Network manager. This file has to be added to your certificate store and is a copy of the certificate file on the file server. This is used by your PC to be able to decrypt email.

If you are opening your email via a webmail browser session (for example, Outlook connection via a corporate URL, in a browser) you will get a red shield message stating that the session is not secure. You are encouraged not to proceed, but to install the correct S/MIME email certificate first as clearly you do not have the same certificate as it is being used to send you encrypted email.





# Extremely short battery life

Less of a problem now with L-ion batteries, but early batteries suffered from the memory effect - the laptop thinks that the battery is, say, 80% charged, so will only top it up by 20% and then stop, whereas in reality the battery is at 10%. Here the battery will be charged only to 30%, not to 100%. The fix for these early batteries was to completely wear down the battery to 0%, then completely charge up to 100%.

Modern batteries do, however, not charge well when power-charged using a fast charger, or receive regular top-ups. The battery was designed to be fully used and then fully charged.



# Overheating

Modern devices contain environmental software to monitor the temperature of core components such as the CPU. If the CPU is running over tolerance, the first thing the PC will try is to reduce the power of the CPU, thereby reducing the amount of heat being generated. This is referred to as throttling as you are reducing the power to reduce the load on the CPU.

Some devices, such as projectors have a cooldown state and will enter this if the device becomes too hot and reaches a point where damage may be incurred. This is designed to stop all essential services and for the extractor fans to expel the hot air from the device.

For smartphones especially, avoid extremes in ambient temperature - a hot location means that the baseline temperature is raised, increasing the likelihood that the device will overheat. However, smartphones do not deal with the cold well at all so temperatures below 0 degrees celsius may cause the device to not function at all.





# Frozen system

A system is considered to be frozen when it stops responding mid-way through running an app or task. You will have to force a restart. On smartphones, this can be done by holding the power (wake) button and the home button for 10 seconds until you see the splash screen appear, at which the device is restating.

If you do not get the splash screen, power off the device and remove the battery. Wait for up to a minute before reconnecting and starting the device.



# No sound from speakers

There are two common causes for this - Laptops and smartphones have a mute button that will cut all sound. There is also a volume control that may be set to 0%.

Do not forget that if you get sound from some things but not from specific apps (for example, YouTube videos are muted) remember that YouTube has its own separate mute and volume control on the player.



# GPS not functioning

As with the mute button, the GPS functionality can be turned off and on. It also is often used with the Location feature to report back your current location to the web server you are connecting with. It is a contained service, managed by the OS so does not require any extra input or configuration from the user.



# Swollen battery

Common with iPhone 5 and 6 phones in particular this is a dangerous problem, where overheating or overcharging has caused the battery to become damaged. The potential for the phone to overheat or to catch fire is present and so if your phone becomes distended or you are concerned about the heat levels being generating, return the device to an authorized reseller for repair, or for a replacement.





# Disassembling processes for proper reassembly

At some point you will have to strip down a PC and rebuild it from scratch. This is usually when you are placing the motherboard, or moving the hardware into a new chassis. These occasions can be fun and as we have already established plugs and sockets are keyed, so you can only plug them in the correct way, so it is very difficult to break the components if proper safety rules are followed. We are going to look at a series of different best practice tips to help you with reassembly.

Never disassemble a PC that is still powered as there are parts that may cause you harm, even shock or death. Always follow the correct safety procedure and never power up a PC on a grounding mat when you are still earthed to the chassis.



# Document and label cable and screw locations

Smartphones and modern laptops / tablets are not user-serviceable, so they are out of the remit of this section. I will concentrate here on the PC that can be stripped down.

There are a multitude of screws, ties and other components, so it is advisable to keep some sort of order as you remove the components. Unlike a mechanical disassembly I would strongly advise against using a screwdriver or any other tool that is magnetized as this may cause damage to the electrical components.

You will first of all notice that there are several different types of screw used in a system build:

- A coarse thread screw with a Hex head, posi-divot is used for the chassis screws.
- A coarse thread screw with dome head, posi-divot is used for the blanking plates.
- A fine thread screw with dome head, posi-divot is used to mount the motherboard to the spacers
- 6-10 christmas tree plastic, or hex brass spacers are used to raise the motherboard from touching the base of the chassis. With hex spacers these have a coarse thread base and screw into the spacer holes on the base plate.
- Four coarse thread, flat-head, posi-divot screws are used to mount the hard drive into the media bay (four for each device).



# Organizing parts

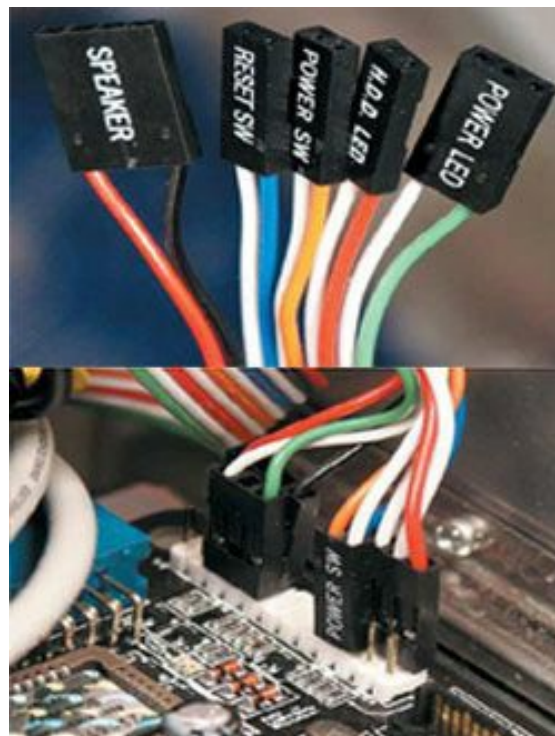
It is advisable to bag and tag each type of screw to ensure that all are kept and are available on the rebuild. For hardware components keep these in separate electro-static bags to avoid damage to the components.



# Referring to manufacturer resources

You might need to buy additional resources to perform the rebuild. For example, cable ties, or wire channel runners are advisable to avoid wires from blocking airflow, being burned on hot components or hitting fans. If you remove the processor and need to remount it, remember that you will need to add thermal paste between the top of the processor and the base of the heat sink block. This is to avoid any air gap and ensure good thermal conductivity between the processor and heat sink.

If reconfiguring the BIOS, also when setting jumpers, or adding the umbilical header block, refer to the motherboard manufacturer manual to assist in plugging the correct wires into the correct pins. Whilst some are keyed, universal chassis use an umbilical with separate pin blocks for each wire pair.







# Using appropriate hand tools

Some technicians place screw glue - a blue / pink liquid into the screw thread first before screwing the screw into position. This, when set solidifies and holds the screw in place. Slightly more torque may be needed to unscrew the screw once it is seated - please bear this in mind and use the correct size screwdriver so that optimal torque can be placed on the divot.



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Troubleshooting Laptops:** <http://www.professormesser.com/free-a-plus-training/220-901/troubleshooting-laptops/>
- **Troubleshooting Mobile Devices:** <http://www.professormesser.com/free-a-plus-training/220-901/troubleshooting-mobile-devices/>
- **Device Disassembly Best Practices:** <http://www.professormesser.com/free-a-plus-training/220-901/device-disassembly-best-practices/>



## **901.4.6 Given a scenario, troubleshoot printers with appropriate tools**

As a first-line support / field technician your work will involve two regular jobs - solving password problems and printer fixes. This chapter is therefore a helpful guide to illustrate a variety of symptoms and faults you will encounter with advice on how to remedy these. We then look at some of the extra resources and tools available for you to replenish, or recondition aging printers.



# Common symptoms

We start by looking at a variety of faults you will encounter, focusing on problems you will encounter with Inkjet and Laser printers that are the most common types, but also produce the most problems.





# Streaks

Where you see bands of color on an inkjet page, the ink has not been uniformly applied. This may be due to clogged nozzles or scratches on the paper itself.





# Faded prints

If you have set the printer to output in Economy mode it will use less ink/toner to produce the image. Also on laserjet systems if the output is evenly faint this could suggest that the toner reservoir is approaching empty.



# Ghost images

If the drum was not cleaned of any previous toner from the earlier printout, then the remnant image will still be present on the next turn of the drum when the current pages image is applied. As a result the latent image is impacted as well as the current image. A broken cleaning blade, or erasure lamps may cause this.



# **Toner not fused to the paper**

Toner is a form of ionized carbon and wax that melts and fuses (bonds) to the surface of the paper once heat and pressure are applied. If there is no heat because the fuser roller is not hot then the toner will not bond to the paper. You can check this by blowing onto the surface of the output paper. The toner will simply be blown off the sheet.





# Creased paper

Paper is passed through the printer in direct alignment (referred to as registered). If it is passed into the rollers askew, there is a likelihood of resistance causing a folding (concertina) of the paper. This is common if two sheets are picked up by the pickup roller, or if the paper is damp, also if there is an obstruction (for example, bits of paper) within the registration rollers.



# Paper not feeding

Laser prints collect paper from a spring tray capable of holding approximately one ream of paper. The spring raises one end of the paper block, so the upmost sheet is biased towards the pickup roller. If the space between the pickup roller and base board is too wide then the paper will not be pushed through and into the assembly. Also if there are only a few sheets in the tray, the paper will not be biased forward and will not make contact with the pickup roller.

Check the pickup roller gap and also that the tray has sufficient paper to ensure that the top sheet comes into contact with the pickup roller.



# Paper jam

All rollers have a pressure sensitivity trip that will cause the assembly to stop to avoid damage. If paper has stuck inside the assembly you will need to open the printer and carefully remove it before any damage comes to the assembly. This is referred to as a paper jam. By applying gentle, but constant pressure on the paper we can gently pull out any stuck paper from in between the rollers.

Upon closing the lid and restarting the printer, the assembly rollers will reset to their original positions and cycle. This clears any debris or bits of paper that may still cause a jam. It is advisable to perform a test print before carrying on with the print job.



# No connectivity

If the data cable to the printer is unplugged, or the print device is not powered, or in offline mode, there will be no connectivity in the status display of the printer object within the OS. To resolve this, check the cable, power on the printer, or go back to online mode (on the printer front panel, on laserjet printers). Once back online, perform a test print from the OS.





# Garbled characters on paper

The laserjet printer uses a print driver that supports TrueType fonts - the fonts are drawn as an image within the OS and sent over to the printer. On non-TrueType fonts, we are reliant on fonts installed on a font cartridge housed within the laserjet printer itself. These fonts correspond to font characters within the OS (for example, Arial, or Times New Roman) and also the specific characters sent to the printer are tied to the language settings on the PC. If I am using a UK Arial font pack in the printer, but my language settings are set to US, I will get incorrect symbols at certain points where the code pages do not match.

If the information being sent cannot be understood at all by the printer, the printer driver is presumably at fault. If all of the characters (including Unicode characters) are garbled, then the fault is that the wrong information is being sent to the printer because the wrong driver is being used. To correct this uninstall the printer from within the Devices and Printers window and reinstall the printer using the correct drivers.



# Vertical lines on page

For laser printers, if the streak is a vertical white line (toner missing from the section) a build up over toner on the transfer corona wire has caused the toner not to be applied to this section of the drum.

For laser printers, if the streak is a vertical black line (excess of toner on this section) a scratch at this point on the drum can lead to excessive build-up at this point. With some models as with the missing line a buildup of toner or dirt on the corona wire at this point could potentially cause this.



The exam is going to have a hard and fast answer so I would advise that you remember corona wire = missing toner and drum scratch = black stripe.



# Backed up print queue

If there are several print jobs in the print queue, but the currently printing job has stalled, all of the other jobs cannot print until the current problem has been resolved. The print queue is said to be backed up. If the problem is software related and the hardware is ready to continue, restart the current job. If the current job cannot be restarted or a page is missing it may be advisable to cancel the existing job at which point the printer continues with the next job in the queue.

Jobs are prioritized based on who sent the print job. Managers have a higher priority than standard users so certain people may jump up the queue. Only the print owner and print managers (people who are allowed to manage the printer queue) can clear a print job.



# Low memory errors

The printer has a buffer within the hardware itself, but this is a small RAM not capable of handling more than approx 1/3rd A4 content, if text. Images certainly cannot be held in the RAM and take longer to be processed. To help with memory issues, we use a print spooler. Here we can slow the transmission of the print data out to the print device at a speed it can handle without overloading the on-board printer RAM. The printer data is spooled (stored in a cache) and released in batches from the spooler to the RAM.

The print spooler service is a very old and unreliable service that may need to be restarted. Restarting the spooler, however, clears any data stored in the cache. With some printers is it better to print directly to the printer, assuming that the printer can handle the flow of data. Modern inkjet USB-connected and network-enabled printers have a much shorter processing overhead and can handle the faster speeds, whereas older laserjets cannot.





# Access denied

Standard end users do not have administrative rights to make changes to the printer object within the OS, such as to cancel someone else's print jobs. The Network administrator can also designate that a user can only print to specific printers. On a network the Printer is in fact an Active Directory object, as a computer, therefore only specific people assigned to that printer can use it. If a standard user adds a network share to a printer they are not allowed to use, they will get an access denied message.



# Printer will not print

It is unlikely that a print device will do nothing, so here the problem is with the printer object within the OS. If this has been set to offline mode then the printer will be at rest and not communicating to the print device.



# Color prints in wrong print color

Inkjet printers use four primary colors: Cyan, Magenta, Yellow, and Black. These three key colors and black are used to create the actual overall color and its darkness setting, for the color dot. If a primary color is missing, it is not applied, for example, to get Olive green we apply 50% Cyan and Magenta, 100% Yellow and 10% black (Key). If the yellow head has run out, you will instead get lilac.

Try it for yourself at: <https://coolors.co/44af69-f8333c-737300-2b9eb3-dbd5b5>.



# Unable to install printer

By default, only domain administrators can install a printer, or AD member objects that have been delegated with the right to install a printer. The user would need the Manage Printers security permission to be applied.





# Error codes

The CompTIA A+ assumes the HP Laserjet to the standard for laser printers. Error codes are displayed on the print device display. With this in mind the error codes you might like to revise are as follows:

- 00: Ready.
- 02: Warming up.
- 05: Self Test.
- 11: Out of paper/.
- 13: Paper jam.
- 14: No toner cartridge installed.
- 15: Engine self-test.
- 16: Toner low.
- 50: Fuser error. Needs servicing.
- 51: Laser scanning assembly problem. Needs servicing / replacement.
- 52: Scanner motor is malfunctioning. Needs servicing.
- 55: Communication problem between the formatter board and the DC controller.  
Will need servicing.



# Printing blank pages

This is unusual. Even with low toner a ghost image should appear. It is more likely that the transfer corona assembly (wire) has broken, or that the High Voltage Power Supply is not working and the drum is not being charged. Given the fact that both of these components are dealing with High Voltage power, you are advised to call an engineer and not to service these for yourself.



# No image on printer display

Some printers have a lockout security feature to prevent tampering. The print device's print display can be locked out--the led display will still be backlit, but no data will be present on the screen until a special key sequence is tapped in. Photocopiers also have a similar lockout - a pin code needs to be typed onto the keypad before the device can be used.



# Tools

In this section, we are going to look at a variety of resources and tools available for you to repair and recondition a laser printer. We will also look at the software tool - the print spooler used to cache data streamed to the printer.





# Maintenance kit

A printer maintenance kit is a collection of new parts that can be installed by the user with minimal effort. It contains new friction rollers (pickup roller and pad), new HEPA filters and toner collection pads, transfer rollers, and fusing assembly. It is also common to find a new imaging drum and toner bay.

Instructions are also provided on how to reset the print counter (printers record the number of sheets printed) given that the installation of the maintenance kit is effectively a complete replacement and reconditioning of the major parts of the printer that will wear out over time.



# Toner vacuum

The problem with using an ordinary vacuum cleaner to clean out excess toner from the printer carcass, is that standard vacuum cleaners produce a static charge that will build up on the image drum - you run the risk of receiving an electrostatic shock.

All of the parts within the toner vacuum are grounded, thereby ensuring that the user cannot receive a shock.

If the printer has just been used it will potentially still be carrying a 600 V charge, which is extremely dangerous.



# Compressed air

A can of compressed air can be extremely useful to remove, or push bits of paper, or toner out of crevices where it can then be swept away. The air can has a plastic straw used to direct the blast of air into specific areas.

- Use a mask when trying to remove toner. The International Agency for Research on Cancer has classified as a 2B carcinogen, or a dust that is possibly carcinogenic to humans.
- Be careful not to expose your skin to the compressed air. This is in fact a solvent reacting as it is released under pressure. The gas is Carbon Dioxide which in itself is harmless, but the solvent if breathed in can have harmful effects and can also burn the skin.



# Printer spooler

Not a physical tool, but a software support function. Printers operate at considerably slower data transfer rates to the PC it is attached to. Data rendered and ready to be sent to the printer is kept in a holding queue referred to as the spooler, which drip-feeds data out to the printer at a speed it can work with.

The spooler itself is old technology and quite often the spooler will expect to hear back from the printer to request further data but become stuck. The print job therefore is incomplete as the spooler is unable to proceed. The solution to this is to restart the print job in the spooler or on more drastic cases to restart the print spooler service. To do this go to the Start Menu | Control Panel | Administrative Tools | Services and locate the Print Spooler Service.

Switching the printer off and on again will may re-establish contact with the spooler, however, the current page's data ready to be printed held in the printer's own on-board memory will have been lost and this will not clear the spooler.





# Exam questions

1. A rack-mounted blade server housed in a 6ft sealed rack enclosure is experiencing repeated, unexpected restarts. The system is working for a few minutes (approx. 10-20 minutes) but then restarts. You check the OS with a Remote Desktop session but can see nothing out of the ordinary. The System error log states when the restarts are occurring, but no probable cause. What is the most likely explanation for the restarts?
  - Answer:
2. A technician reports that a server mounted in a cabinet is making very loud 'jet engine' noises. You connect to the server using a Remote Desktop session but cannot see any problems within the OS. What could be the cause of the noise?
  - Answer:
3. A user reports that they have had their PC for some time. It has several hard drives and has had many OS systems installed over the years. However, after working on the BIOS he notices that some of the OS systems installed are not available to him. Why may this have happened?
  - Answer:
4. The user pulled the Ethernet cable out of the PC without taking care and has snapped the locking lever on the RJ-45. They are concerned that damage may have occurred to the port itself, however a PING test reveals that test packets are successfully sent using PING 127.0.0.1 and also the NIC's IP address. Are there any further tests which can be done to test for damage to the port?
  - Answer:
5. A user reports that when booting the PC they receive a SMART error. What does this signify?
  - Answer:
6. A technician is trying to install a new hard drive into their PC. They have been told that it needs to be installed underneath the media bay but they do not know where that is. How would you advise them?
  - Answer:
7. Name 5 things that can be done with the DISKPART tool which cannot be achieved via Disk Management.
  - Answer:
8. What is an artifact?

- Answer:

9. A user reports that their screen is flickering. Horizontal black lines are showing and the image appears to be unstable. What is the cause of this?

- Answer:

10. You are connecting the PC to the Enterprise network, but work has been done on the DNS server. Your PC is manually configured. You notice that it takes a long time to access network resources and in most cases the request times out. You also cannot connect to the internet but can PING local PCs on the same floor. What can be done to correct this?

- Answer:



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Troubleshooting Printer Problems:** <http://www.professormesser.com/free-a-plus-training/220-901/troubleshooting-printer-problems-3/>
- **Printer Troubleshooting Tools:** <http://www.professormesser.com/free-a-plus-training/220-901/printer-troubleshooting-tools-2/>



# Summary

This section is an invaluable list of repairs and problem-solving techniques that you can use to locate and troubleshoot both hardware and network configuration problems. For Networking, read this chapter alongside the second chapter that introduces each of the network hardware components.

You should now, once you have understood this chapter, be able to troubleshoot common system device problems relating to the motherboard. You will be able to identify problems relating to hard drives, or RAID configuration and to formulate a remedy. If given a certain scenario you will be able to detect problems with display devices. Given a scenario you will be able to identify and correct problems with both wired and wireless networking. Given a scenario you will be able to identify and possibly resolve (where user-serviceable) problems with mobile devices. Finally and importantly, you will be able to detect and resolve printer maintenance problems and use the correct tools to do so.



# Next steps

At this point you should now have the knowledge to consider preparing for the first exam - CompTIA A+ 220-901. There will be some crossover with material for the second part (the 902 exam), but you should have sufficient knowledge to be able to now work on preparation materials such as practice test questions.

I personally use the <https://www.measureup.com/default.aspx> website. Although you have to pay for access to the questions, the questions are legitimate - they have been put together by a panel of industry experts and are approved learning materials. Measureup is owned by Pearson VUE - the company you will need to take your exam at, so I trust their judgment to provide the best learning experience for you to proceed.

When I take CompTIA tests, I learn in study mode. I take 5-10 questions from one domain at a time. I have the engine set to show me the correct answers immediately. If I get it wrong, I read the answer statement in which there is a detailed explanation why the answer is right and the other ones are wrong, with links back to online reference material, so that I can alter my learning and take on board the reasoning.

Once I'm happy that I am competent with the questions, I take a full test in study mode. When my score is approx 70-80%, I then take a test in Certification mode. This is an emulated actual test environment. It is a timed test, exactly how it will feel in the exam room. Aim get and pass the cert exam with 80% or higher - twice. If your line manager is paying for your exam voucher they may need evidence that you are ready to proceed with the exam - this pass in Certification mode is your evidence.

On the day of the exam, do not be distracted, and make sure that you are well hydrated and ready for the test. Do not take anything into the exam room other than the pen and paper / board supplied by the centre. Keep your personal belongings, especially a mobile phone in the locker located at the centre. Make sure that you take photo ID (two forms of ID usually) with you as you will need to identify yourself. When you sign in, you will have your photograph taken - this will actually go on your test results sheet.

When you complete the exam, you will be given a test result sheet with your score. It will list on the sheet if you have passed or failed to reach the target score. If you need to do further work notice the domains listed - these are the sections you still need to develop.



Once you have passed both A+ exams you will need to claim your certificate from the CompTIA Transcript site. Details of how to do this can be found on the following link: <https://certification.comptia.org/help/certificates-credentials-transcripts/credentials/create-a-transcript>.

In the next chapter, we will start part two of our journey in which our focus will be on the various OS and applications used in a variety of devices.



# Introducing part 2 - 220-902

The first part of this book is simply a sponge exercise. Part I requires that you memorize a lot of technical information - that you can identify parts and components, customize them, and perform rudimentary practical changes.

The second part of the A+ is not so challenging and is more like what you are used to as your 'day-to-day' support. Most of the things you will need to fix will be system tweaks within the Operating System, so here we are going to look at how the OS functions. From an exam perspective, we are going to take a look at some of the traps and pitfalls you will encounter--are you being asked to roll back; to use a system restore? To use a backup? How should a problem be fixed? What is the easiest and less obtrusive fix? You will need to not only give an answer that is sensible, but one that is not 'overkill'.

You will need to already be able to demonstrate that you can:

- Assemble components based on customer requirements
- Install, configure, and maintain devices, PCs, and software for end users
- Understand the basics of networking and security/forensics
- Properly and safely diagnose, resolve, and document common hardware and software issues
- Apply troubleshooting skills
- Provide appropriate customer support
- Understand the basics of virtualization, desktop imaging, and deployment

The 902 content is broken down as follows:

1.0 Windows Operating Systems	(29%)
2.0 Other Operating Systems & Technologies	(12%)
3.0 Security	(22%)
4.0 Software Troubleshooting	(24%)

5.0 Operational Procedures	(13%)
----------------------------	-------



# Windows Operating Systems (902.1)

Arguably the most significant part of the 902 exam is the Windows Operating System domain. This has been quite contentious as CompTIA is **vendor-neutral**, but the argument is that Microsoft's Windows system is the most used by home and professional users. IT Technicians will also gravitate from the client to the server OS as their experience with the wider network increases. To this end CompTIA have now added a later chapter covering Apple and Linux systems and by so doing have covered most of the systems in use. Not all, but a good understanding of how these work, with Windows knowledge underpinning your learning is a great approach to take.

We will first look at the Windows systems from Vista to 8.1. I will also mention and in fact use screenshots from 10, but currently at the point of writing 10 is out of scope. I have however referenced material which is also relevant for 10 in an aim to future-proof the book for the next few years as the exam bank adapts to accommodate the usage of 10. We then look at specific scenarios, considering how we can boot into the system. We then focus on the Command-line tools available to us before a lengthy and detailed look at the GUI tools available. We then focus specifically on the Control Panel toolset, then specific network elements and then finally maintenance procedures specific to Windows.



# **902.1.1 Comparing and contrasting various features and requirements of Microsoft Operating Systems (Windows Vista, Windows 7, Windows 8, Windows 8.1)**

You'll find that given your background you will either favor supporting Macs, Linux, or Windows. CompTIA needs you to be an all-rounder and to put political (with a small p) differences aside. What do I mean by this? IT technicians are keenly and dearly passionate about the software they manage and equally 'buy in' to the collective community. The difference politically between Windows and Linux is due to the nature of open source and anti-capitalist sentiment. Like it or not Microsoft is a large and successful company. Over 85% of users are using Microsoft. It just is and it works.

Linux is an opensource system. This means that its core code is available to read in the public domain and anyone can tweak it and be part of a community of coders. Linux is free (there is one commercial version, but in the main it is free) and Linux enthusiasts feel that other software, such as Microsoft should be free. This is in part why there is such tension. Apple's systems are very expensive and are scaled down. Out of the box the Apple system is not designed to join a domain and does not have most of the security features built into the Microsoft platform. Apple is considered elitist as the machines are very expensive and are easy to maintain. However, the truth is that Apple's OS X platform is based on UNIX. Linux is a UNIX system as well. Microsoft's DOS (the old underlying code to the older Windows systems) is a lite version of UNIX. They are interlinked.

History-lesson aside, you need to ensure that you embrace all technologies with equal fervor and not to shun a particular one, at this point in your career. You will likely favor one system because you will be servicing that system as you specialize, but you are not at that point yet.

So coming back to Windows, we are assuming that you have used XP extensively so every reference to other systems (Vista, W7, W8, W8.1, or W10) when we refer to existing tools, will look at user interface changes, new menus, but in essence how an



action is performed has not changed. There will be 'in homage to XP' references through this book and this is deliberate, so do ensure that you are familiar with the systems. I will however also focus heavily on the new tools available from Vista onwards.

Download a copy of the evaluation ISO from the Technet Evaluation Center (<https://www.microsoft.com/en-GB/evalcenter>) and set up a series of virtual machines so that you can contrast like-for-like the different systems for yourself.

Windows 10 is out of scope for the exam, however, the exam bank is constantly being added to. If it is mentioned in an exam question assume that the question is not asking you to have researched any differences between Windows 8.1 and Windows 10, rather that the function you are trying to achieve would have been actioned the same way in Windows 8.1



# Features

The Windows system is packed with features and each new version promises key advances. Later editions have focused on functionality and the user experience allowing you to get more done. The motivator of course is the long-standing comparison of the Microsoft system with Apple's OS that just works. It's simple, graphical approach has been something Microsoft have also tried to emulate. Later motivation comes in the form of Microsoft's launch of the Surface, which can operate as both a notebook laptop and a tablet. Windows 8 onwards editions are designed with the productivity possible from a tablet in mind.



# 32-bit versus 64-bit

The original PC used a 32-bit architecture with some parts of the motherboard also actually using 16-bit and even 8-bits as well (for example, ISA slots). Over time the Operating System became more sophisticated as we realized that more bits led to greater processing capabilities. Around 2005 - 2010 the 32 and 64-bit architectures ran in parallel and it was not until Server 2008 Service Pack 2 a decision was made to abandon the 32-bit architecture entirely.

Client-wise Windows XP was the first to have a 64-edition and parallel architecture releases have ran for several years. At present the 32-bit system is being phased out. Windows 10 is designed with the 64-bit version in mind and most laptops and systems built presently are 64-bit.

How do we determine if I have a 32 or 64-bit system? What am I measuring here? The architecture refers to the type of processor you are running and subsequently the motherboard designed to support it. We have 64-bit worth of data lanes connecting to the rest of the components on the board.

Driver-wise it is worth noting that 64-bit drivers will only work with 64-bit hardware. If you are using 32-bit hardware (for example, an old audio card) it will physically connect, but will need a 32-bit driver in order to communicate with the device--a 64-bit driver is not 'backwards compatible'.

64-bit drivers cannot be used on a 32-bit architecture for the same reason - it was not intended for this hardware system.

With servers it is worth noting that drivers (from Server 2008 Release 2 onwards) have to be digitally signed - we use the driver provided by the original manufacturer that has a confirmation code added to it to prove that the driver file is legitimate. This is to avoid adding potentially virus-ridden drivers onto a system.

This does not sit well with the Linux community. Here, drivers are open source- the community adds and extends the code providing variants with extra functionality. This works fine so long as the community have tested the code prior to its release to the public. Finding a driver may therefore need some research and Linux drivers may not always be available from the manufacturer. Getting the manufacturer-approved driver is therefore often the more sensible and secure solution.

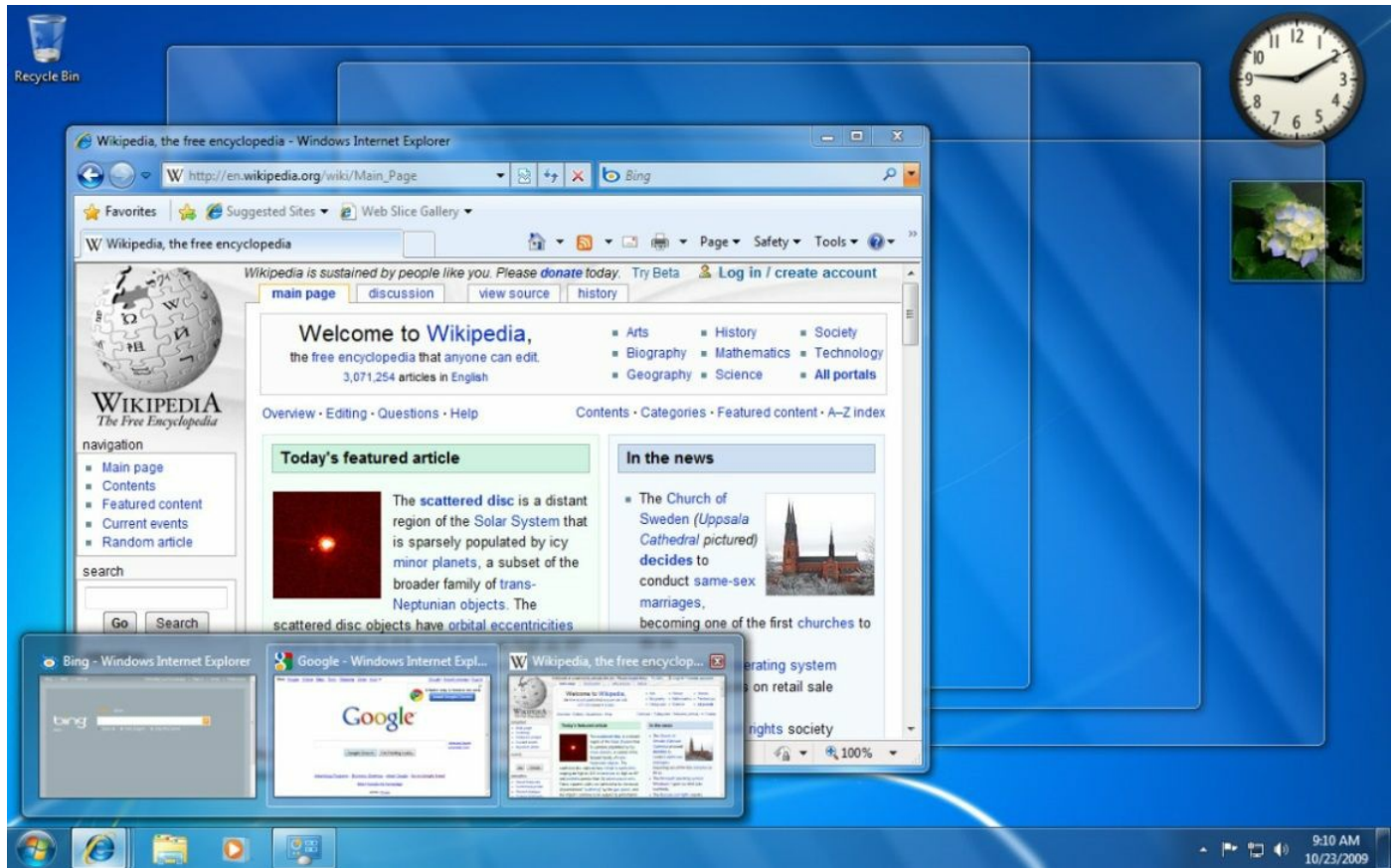




# Aero

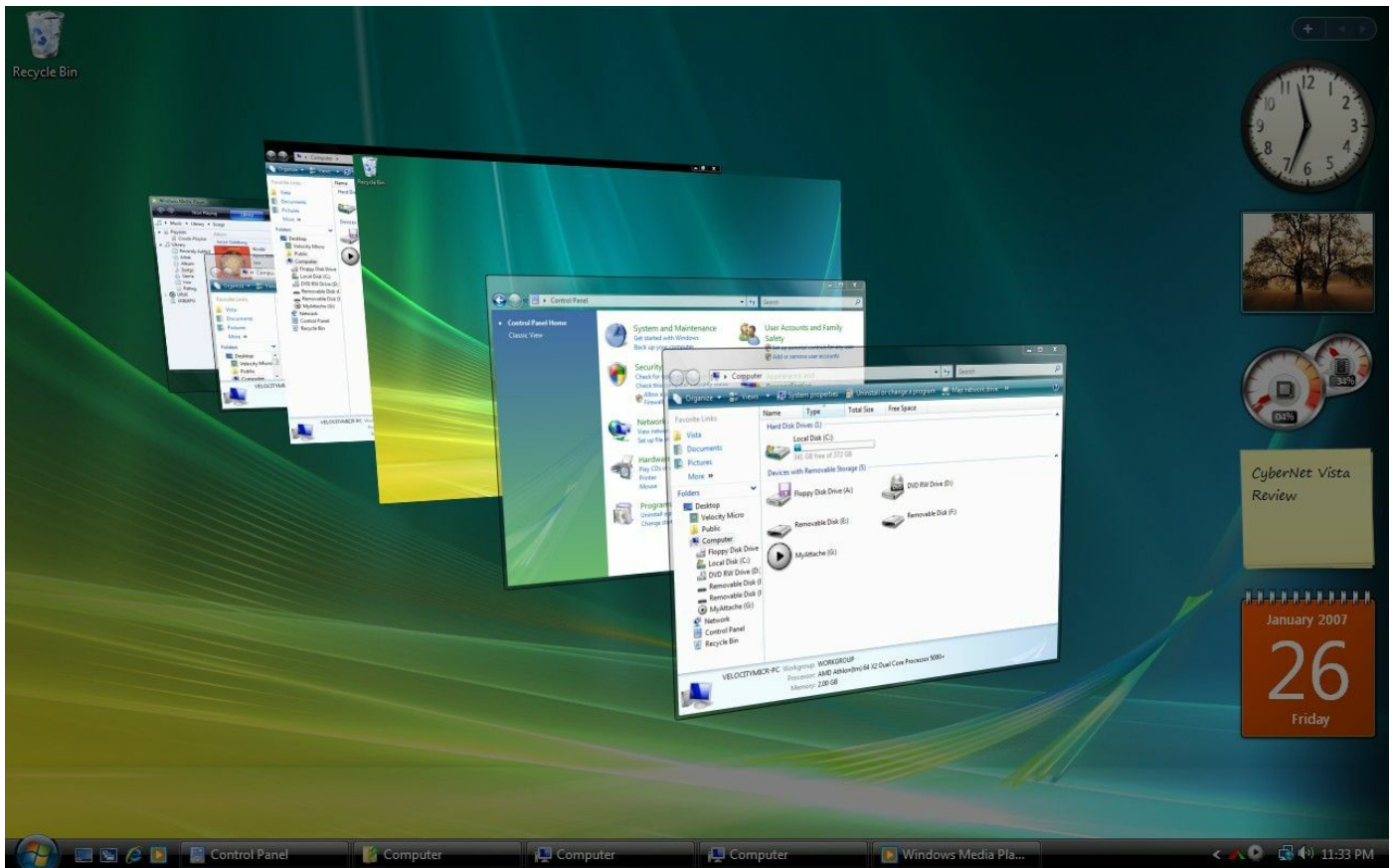
Aero is a family of display features built into Windows systems from Vista onwards:

- **Aero Glass:** Windows XP used a forms display theme called Luna. The design team this time wanted to include translucency into the forms, so the Glass theme was developed.



- **Windows Flip:** This feature allows for a live preview of the open applications and allows you to cycle through these applications. It was only available in Vista and 7, but was removed in 8 and 10.





- **Aero Peek:** It is available from 7 onwards, by hovering the mouse over the taskbar you now get a thumbnail of the live application. If you have several applications open on the same screen, by then hovering over the thumbnail the main screen will change and instead show you a preview of that app.



I find this extremely helpful where I want to check on the status of a job, for example, installing an application and want to see how far into the installation it is. I often also work on Microsoft Online Labs and have the instructions on a PDF document. When I am working in my office, that is fine as I have two monitors, so can have the instructions open side-by-side, but if I am working away and only have the one monitor (for example, on my laptop) then I can use Peek to read the next line of instructions without having to Alt + Tab every time to get back to my lab.

- **Aero Snap:** It is available from 7 onwards Snap is invaluable. Here, you drag the window by its title bar and place it on one of the sides of the screen. The window will automatically resize to fill half of the screen.

I regularly use Snap when I need to move files from one location to the other. I open two File Explorer windows--one with where the files



currently are and the other shows where the files are to be moved to. I then can drag and drop the files. This is much quicker, easier (liked by Apple users who are already used to this functionality) and does away with the more tedious Move option built into File Explorer

- **Aero Shake:** It is the ability to minimize all other open windows so that you can concentrate on the active window. To do this move the mouse to the title of the active window and move the mouse vigorously from side-to-side. The app will maximize and everything else will minimize.



# Gadgets

Gadgets are not popular now. Gadgets were used on the other Operating Systems to improve functionality and were a stop-gap measure to add live data to the desktop. The problem was that the Vista (where gadgets were first launched) was quite a bulky system and did not deal with gadgets well. Gadgets increased memory usage and slowed down the system.



Ironically these problems were addressed in Windows 7 before Microsoft then changed its focus, shifting over to a more diverse OS that could support dynamic data and touch-screen UI, for use on tablet devices. This became Windows 8 and the Start screen.



# User Account Control

While XP was a stable system, if attached by a virus such as a macro virus, the virus code would be executed with user permissions. If the user was an administrator (and on home systems they invariably were) the code would have free reign over the OS to make whatever changes it liked.

Macro viruses sent movement commands to the mouse pointer, clicking and performing a series of actions. This was a common type of virus that did affect a number of XP systems.

To stop this, **User Account Control (UAC)** creates a second security environment. When an action such as a request to install a program is triggered, the user environment is paused. Overlaid is a glass pane where the second security environment will prompt the user to give permission for the action to run. Depending on your setup you will either be asked to approve the request, or may be asked for your login credentials. Not only does this provide security and peace of mind to the end user, if this was virus-triggered code and you did not action this step, you may realize that something is wrong and will have this chance to stop the virus in its tracks.



UAC is in fact a background service and should always be left on. Within Control Panel there is a User Account Control page that allows you to reduce the amount of notifications you receive, allowing some low-key tasks to run and only alerting you for significant system changes. Moving the slider to never notify means that all tasks are

allowed (not good!), but it is important to know that UAC is still active, just not really doing anything.





# BitLocker

BitLocker is a full-disk encryption system. It can be used in conjunction with file encryption systems such as 7-ZIP or Windows own EFS, which is native to the system. It was launched with the Ultimate / Enterprise versions of Vista and 7 also the Professional and Enterprise versions of 8, 8.1, and 10.



There are several changes to BitLocker:

- The Vista version worked per volume and encrypted the Volume. It did not do anything to unused space on the disk.
- Vista SP1 used a graphical tool. Up to that point we used a command tool: `manage-bde` to set up BitLocker and still use it to mount a BitLocker volume.
- Windows 7 supports the encryption of removable drives. This functionality is referred to as BitLocker to Go. For Vista and backwards capability for XP, a BitLocker To Go reader was needed to read data from these drives.
- Windows 8's BitLocker can actually offload the process of encryption to the storage devices' own hardware.
- With Windows 8 BitLocker can be controlled through PowerShell.
- Windows 8 also supports the encryption of a bootable image, referred to as Windows To Go. This is used in the Enterprise environment so that contractors can access the network using a standardized image supplied by the company whilst they are on site. No data can be stored to the laptop's own internal hard disk while Windows To Go is in use. All files have to be saved back to a file server. The drive mapping for this would have been set up on the Windows To Go configuration.
- In **Transport Operation** mode, the cryptographic key used by BitLocker is stored on the motherboard's **Trusted Platform Module (TPM)** chip. This key is used to encrypt and to decrypt code. This certificate file is therefore symmetric - it is fast and contains a complex algorithm.

- **User Authentication** mode supports the use of a PIN code, or other device such as a biometric scanner before the volume will be unlocked.
- USB key mode supports the EAP standard, so it also supports CAC ID card readers and biometrics. Here a USB key containing the password as a file has to be inserted before the machine is booted.
- BitLocker can protect the system at an extremely low level. BitLocker integrates well with UEFI, so the BIOS can also be encrypted, stopping low-level attacks (for example, Rootkits).
- As of Windows 8.1 BitLocker could be used to offer Full-disk encryption. Here the entirety of the disk is encrypted whether used or not. The problem is that you have the option to switch modes between full disk and volume encryption. If you have a dirty (previously used) disk and make a new volume on there that only takes up a small portion of the disk, if you decide to encrypt the volume the remaining space which, although now unused is not encrypted, may be read by a low-level reader.



# Shadow copy

Shadow copies have been around for a very long time. Imagine that you are working on a Word document and periodically save the same file using the File | Save button. You would think that the original file is updated and so some extent you are correct, but Shadow Copies does more than this--each save is stored in a different area of the volume and marked with a version reference and timestamp. If you have made a major mistake and need to roll back to a previous version, you can access the volume's shadow copies and retrieve all of the saved versions.

The process of retrieving the older file is quite labor intensive. The end user has to look at the timestamp from the list of previous versions and then select which file will replace the active one.

Shadow copies are linked to the System Restore function on most versions of Windows, which makes the Restore function now quite important. Each day any new saves are stored within the restore file, so the version you want to retrieve is tied to the available restore files. By using the Previous Versions tab you can track back and restore the one you want to go back to.

The Previous Versions tab can be found within the properties pane for the affected file. The file has to be saved onto the volume we are seeking to protect.

The Previous Versions tab was removed in Windows 8, but restored in 10.



# System Restore

System Restore, as a tool has been around for a long while. It was marketed as a key product in Windows 95 and features in the Windows Millennium Edition promotional video (<https://www.youtube.com/watch?v=kiNWw7h8cEU>).



Each day (or whenever you set it to), the system will take a back-up of all changes. This includes updated drivers, installed app files, and so on.

Actually this isn't entirely true. The old files are backed up allowing you to restore back to the originals and roll back to the point in time before you installed the problematic app or driver that is causing your system to become unstable. Registry changes (the original entries) are also backed up.


Shadow Copies (the old version of the file) also feature in the system restore backup file.

For it to work you have to enable System Restore, check the volume you wish to restore (at least your OS drive should be protected), and specify an amount of disk space System Restore can use.

When you use System Restore you will be presented with a calendar showing key milestones on certain days. By selecting a date we roll back everything to that date. User files that were not counted in the system restore point are not changed, so this is not to be used as a backup solution.

System Restore

Restore your computer to the state it was in before the selected event



[How do I choose a restore point?](#)

Current time zone: Central Daylight Time

Date and Time	Description	Type
4/7/2011 3:36:05 AM	Uninstalling Outlook 2010	Manual
4/7/2011 2:19:11 AM	Windows Update	Critical Update
4/7/2011 2:17:58 AM	Installed SyncToy 2.1 (x64)	Install

☐ Show more restore points

Scan for affected programs

< Back

Next >

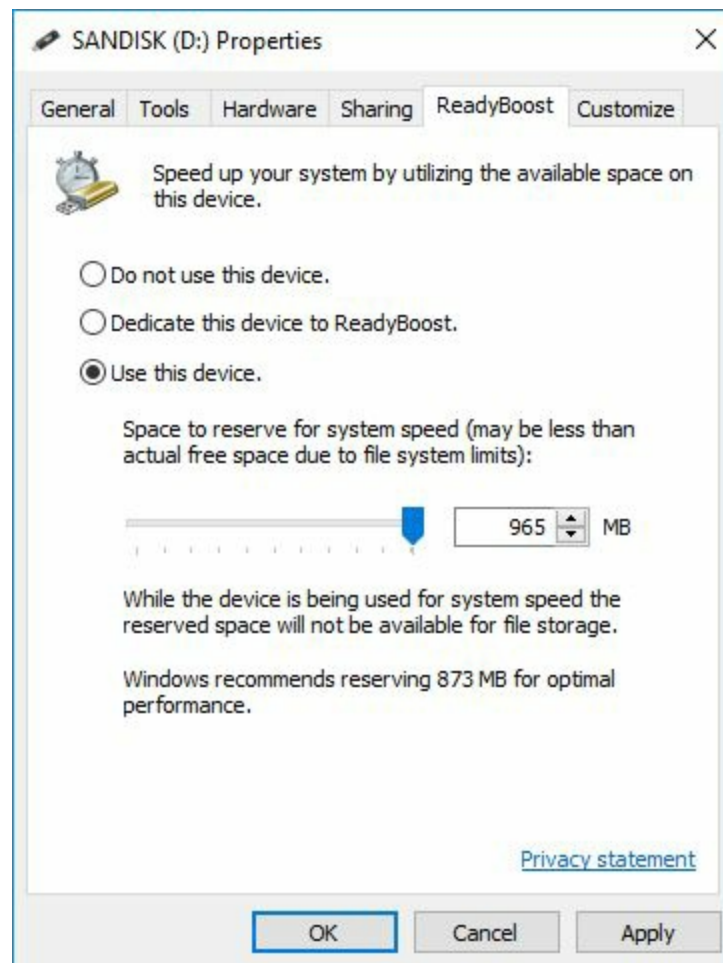
Cancel





# ReadyBoost

One problem with Vista was not so much the fact that the Operating System footprint was quite large, but that the hardware at the time was still relatively small in data terms, also slow to read and write to. One solution was to make use of the fact that USB2 removable drives were effectively Solid State Drives with extremely fast read/write speeds. ReadyBoost gave us the functionality to add extra RAM in much the same way as a swap file is used on a Hard Drive, but with much greater access speeds. The OS can be tricked into thinking that a system with only a few GB of memory actually had more. While not a perfect solution it was a good stop-gap breathing life into older laptops that otherwise would not have run Vista or 7 at all.



As Windows 8 was a much smaller footprint, data-wise but used different architectures, the demand on the processor reduced (in fact a variant of Windows 8, Windows RM is designed for ARM chips and smartphones). ReadyBoost became less needed, but is still available.





# Sidebar

The sidebar was a transparent section that sat over the desktop in which you could place gadgets. In Vista the sidebar was located on the right side of the desktop. With 7, gadgets could be located anywhere at all on the desktop. The Start screen with its live tiles was seen to be a replacement to gadgets.



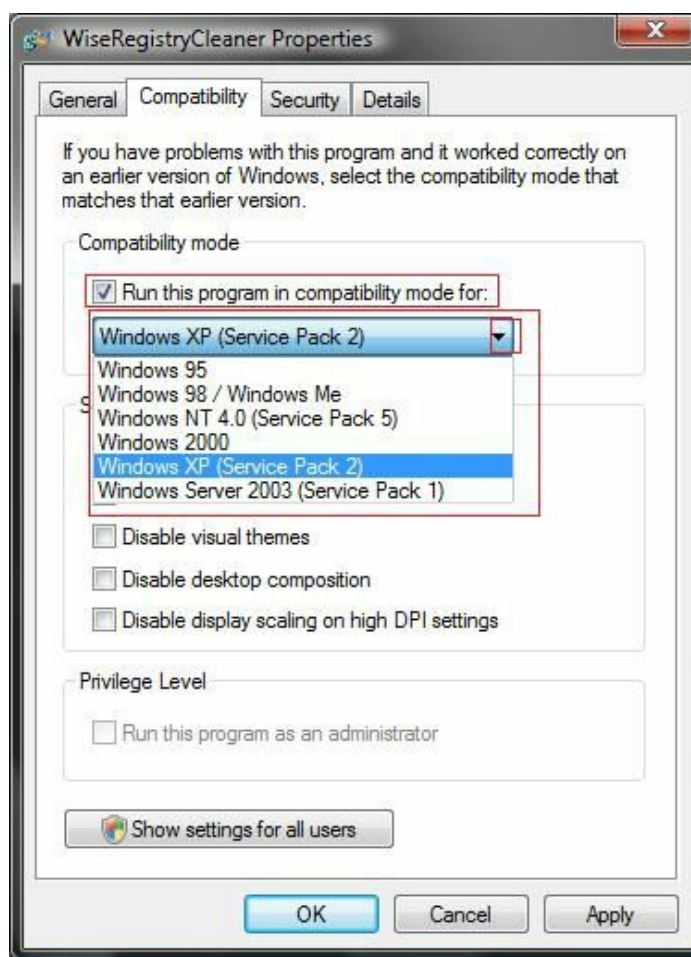
NB: Gadgets are now not considered to be effective, productive, and actually slow down a system.





# Compatibility mode

Vista's underlying code architecture is significantly different to XP, although functionality - how code was executed and accessed can be emulated as if you were running the app on the earlier system by using a properties tab called **compatibility**. This even came with a wizard that would help you to decide if the app was not working and if further measures needed to be taken. In essence we are tricking the app into thinking that it is on an XP machine. The main problem with apps not working was due to UAC as permission was not being given for the app to run. By enabling UAC you are only changing the security profile on this app and not the whole system.





# Virtual XP mode

However, there are times where mimicking the earlier OS just doesn't work. For these occasions Microsoft have supplied a downloadable image known as Virtual XP.

Windows 7 uses a scaled down version of Hyper-V client known as Virtual PC. This was not natively available and had to be downloaded (<https://www.microsoft.com/en-us/download/details.aspx?id=3702>). The VHD file is unique and subsequent replacements to VPC in Windows 8 and higher use the same schema of VHD file as in Server 2012. In fact it is possible to use a VHD file made for Windows 8 on Server 2012's Hyper-V and vice versa (there are some exceptions to this especially when using differencing disks, but the Windows 8 client Hyper-V is almost identical to the server Feature).

The Virtual XP VHD is a vanilla build of XP, ready for use. Simply add a network share to the host PC and install the problem app onto the XP environment instead.

This was a fair solution for home users, that is, if a game would not load in Vista, but not an ideal solution for an Enterprise environment. A better solution for the Enterprise user would be App-V (where the app is run on a remote server and the output is streamed to the host PC).





# Windows Easy Transfer (WET)

Windows XP came with a tool referred to as the Files and Settings Transfer Wizard. This would take a user profile, its configuration settings, and all related documents pertaining to the user and archive them in a transferable file.

The problem is that the underlying architecture in fact how User profiles work under the bonnet has significantly changed with Vista. For example, the **Security Accounts Manager (SAM)** database will not accept user profiles from XP, so instead a new user account has to be created and any security properties set (for example, which shared folders the user has access to and also the level of access) would have to be ported over from the XP environment.

The Vista installation DVD and also the Vista, 7, and 8 systems have **Windows Easy Transfer (WET)** installed. WET is a wizard that will guide the user through which user profiles are to be captured.

The WET process captures user documents and files, configuration settings, security properties assigned to the user, and any other user-related information found in the registry.

The idea is that you need to run WET from the disc on the XP machine, create the backup file using the WET wizard, and then transfer the file via a pen drive, or external hard drive on to the new machine. By double-clicking the file on the new machine (or running WET and select the import sequence) any captured user profiles will be recreated on the new machine.



NB: As mentioned earlier the account GUID will be different on the new OS. It was also possible to use a WET cable to directly transfer the file from the old PC to the new PC. This was a USB transfer cable sold by Microsoft to perform the WET transfer, however, you could do just as well to use an external pen drive. WET has been discontinued with Windows 10. With Windows 8.1 you cannot directly import a profile from Vista. If you wanted to migrate a profile from XP to 8.1 you would have to do this via 7. User profiles cannot be migrated across platform - you cannot import a profile from a 32-bit system onto a 64-bit system and instead will have to recreate the profile and import the files stored.

For Enterprise users WET is not a good option as you often have to upgrade several user profiles at the same time, as a batch job. To do this the downloadable **Microsoft Deployment Toolkit (MDT)** comes with the **User State Migration Tool (USMT)** that can bulk process a lot of user accounts in one go. USMTv2 was available in Windows 98 and was used to transfer to XP. The version we will concentrate on for the CompTIA is USMTv4 that is used to migrate from XP to Vista. USMTv10 can migrate from XP direct to W10, whereas WET cannot.



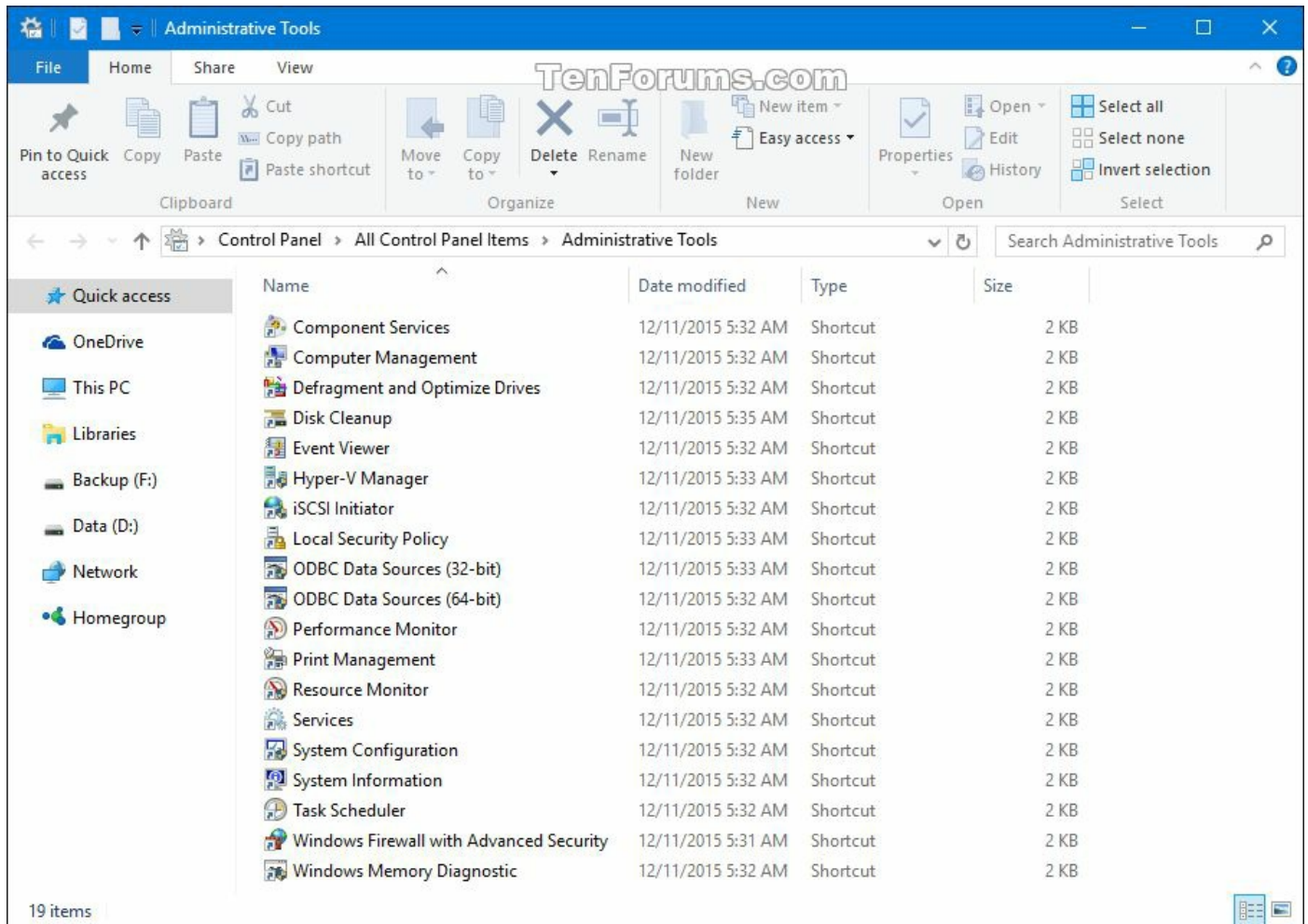
# Administrative tools

This is a selection of 23 items (on W8.1) that are used to perform maintenance or other low-level system changes. They are not designed to be used by the end user as they may inadvertently damage their OS:

- Component Services is a list of all active COM+ modules. These are the low level drivers and communications mapping between the OS, Apps, and devices.
- Computer Management is a 'swiss army knife' of common tools used to inspect a machine.
- Defragment and Optimize Drives accesses the native defragment tool built into the OS.
- Disk Clean-up is used to access the native clean-up tool built into the OS.
- Event Viewer is used to access the event logs.
- There are two IIS managers used if the system is hosting web services or websites.
- iSCSI initiator is used to manage any iSCSI hard drives attached to the PC.
- Local Security Policy is an extensive set of definable configuration parameters affecting the behavior of the OS.
- ODBC data sources (a 32-bit and separate 64-bit menu) lists any database connections you have set up on the system.
- Performance Monitor runs a graphical tool allowing access to a large variety of performance counters. These can be displayed on a graph, or as a dynamic report. You can even save data over time - it is good practice to, once you have built your OS take a collector set with key performance data to show what 'good' looks like. This baseline data is used as a benchmark so that you can compare how the system has adjusted over time.
- The Print Management tool is a Print Server GUI allowing me to add, share, and otherwise manage print devices attached to this PC, making them available to other users across the network. From here I can see the print queues on all attached printers.
- I often describe Resource Monitor as Task Manager on Steroids. It is a more detailed and graphical equivalent to Task Manager showing considerably more detailed information concerning processor use, memory, network transfers, and disk activity.
- The Services tool gives you access to see all installed background services. From here you can start or stop a service, but also adjust when a service is triggered - should it be started immediately during the boot process? Should the system wait

until the user has logged in? Should it be started by the user manually? What context should it run - which user, or computer account should be used to run it? Also if the service fails what should be done? Should it be restarted straight away, or perhaps trigger a message to the user?

- System Configuration is a useful GUI allowing you to see the current boot settings, the services loaded by the existing user and the apps that loaded at startup. You can make changes here to stop additional or superfluous services and apps from loading, tweaking the system, and hopefully speeding up load times. You can also access the 17 other common tools that are often used by system support technicians.
- Would you like a service to start at a specific time, or be triggered to start when something happens? Task scheduler is commonly used to set a daily backup to start at a specific time but can be used to trigger other events.
- Windows Firewall actually accesses the full GUI from where you can set firewall rules to open / close a specific port, trigger a port change when the user accesses an app, or to set up a secure tunnel, for example and IPSEC tunnel between two PCs.
- Windows Memory Diagnostic is a little misleading. This is also available on the install DVD and a Windows RE DVD should you decide to make one. The Memory Diagnostic tool will tell the system to run a memory diagnostic the next time the system starts and will ask if you want to do this now, in which case the system will restart. In order to run a memory test only a small, minimal OS is loaded and from here most of the memory addresses can be accessed and tested.
- We have also a PowerShell Command Prompt and the ISE PowerShell editor from which we can run PowerShell commands.



Learn how to call these from the command console. Each of these are **Microsoft Console (MSC)** files, so `Services.msc` would load the Services pane. Learn these by right-clicking on the shortcut and look at the filename in the Properties pane. Test it by using the Windows Key + R to bring up a run box, or in PowerShell / Command Prompt run the file. As the Windows System path is hard-coded into the PATH environment you do not need to change the directory you are in to be able to run the command. I regularly use `SERVICES.MSC` and `MSCONFIG.EXE`. Note that some are EXE files and some are console GUI files. Note that the Registry Editor is not in this list. This is deliberate as entering any configuration directly in the Registry is not something you want an end user to do. The command however to get into the Registry Editor is `REGEDIT`.





# Windows Defender

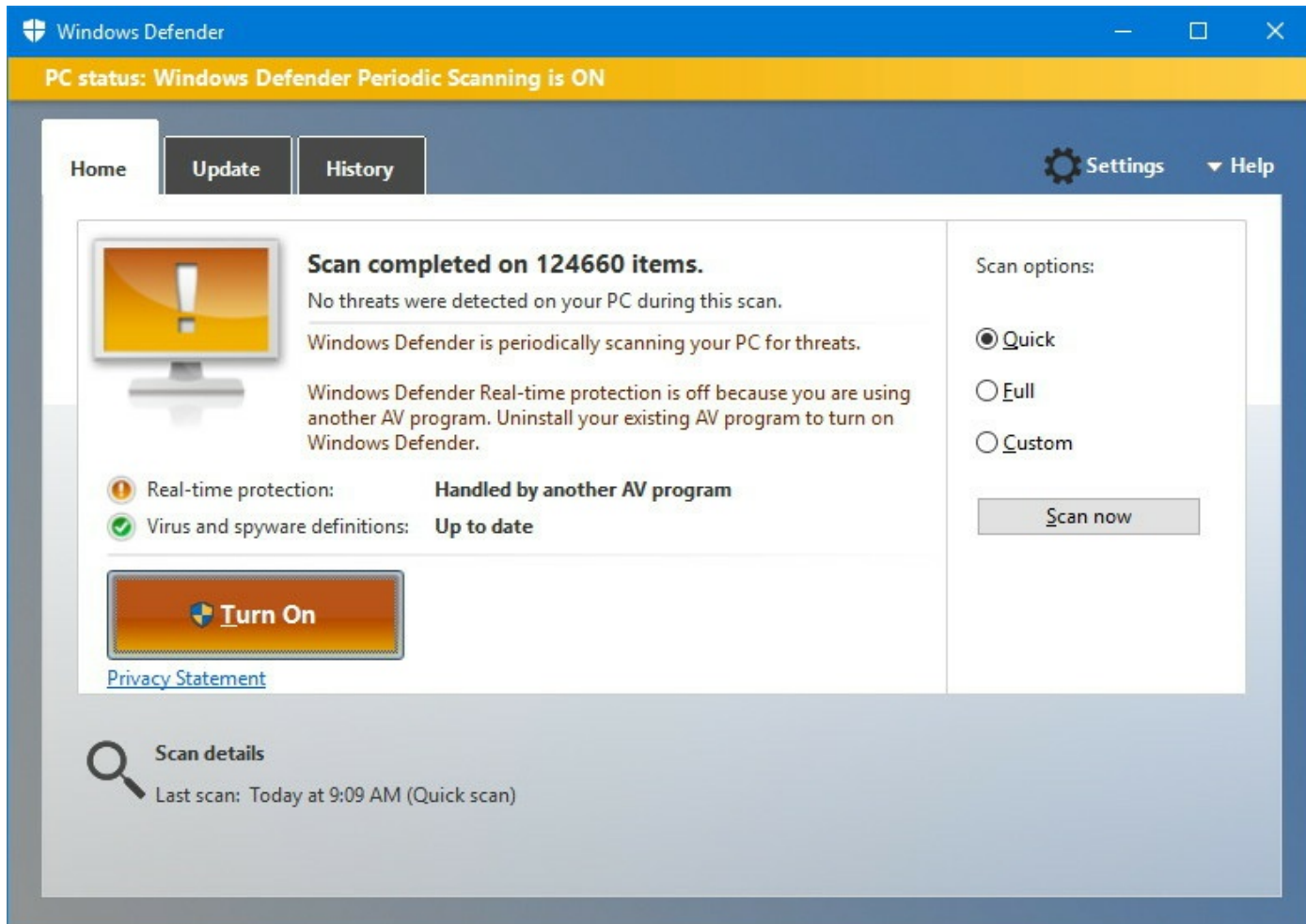
This is an interesting one. Windows Defender was available as a download for XP Service Pack 2 and onwards, but is installed natively on Vista. It used to be part of the Microsoft Security Essentials update but as I say, it is now native to the OS. It is a good, reliable anti-virus program to rival McAfee, Sophos, or Norton.

The short answer is that so long as you keep it up to date, Defender is a good solution for the home user and for most SOHO businesses. It does not protect against Malware (annoying programs or advert pop-ups), so other software such as Malwarebytes Antimalware (<https://buy.malwarebytes.com>) is recommended, although you will now notice that a free version is no longer available other than as a 14-day trial.

For Enterprise users antivirus software such as Kaspersky or BitDefender would be a better solution than Defender as the Defender virus dictionary is not as up to date as I personally would like, in comparison to these two. However, Defender is free and catches most threats well.

A common problem, and you will see this with home-use OEM laptops is that a user will be sold a laptop with a rather bloated system image (I was cleaning down a Sony VAIO yesterday and wasted two hours of my life removing bloatware from it.) may come with software to trigger a trial account for third-party virus protection. It may already have a 'life' protection solution such as McAfee installed as well as Defender. That is two programs that both offer Real-time protection. That means that if you want to access a file it is first scanned for problems against the large Defender database, then again it is scanned against McAfee's database before the file opens. And you wonder why the system is running slow?!

Only have one virus protection program running on the client PC as several will cause significant performance issues for the user who may blame it on the hardware and not realizing that they are unnecessarily overworking the system.





# Windows firewall

In fact there are two GUIs here. The basic Windows Firewall allows you to enable and set which profile you are using. Each profile (there are three underlying profiles) can be configured with different rules, or you may decide to make a rule to run across all of the profiles.

The main profiles are:

- **Private Networks:** These devices are trusted. You may be part of a SOHO workgroup, or domain.
- **Guest or Public Networks:** Other devices on this network are not trusted. The system is to be treated as an individual cell and not to share its data with other devices on the same network. This applies when in a public area such as an airport or cafe.

Underneath these are three security profiles:

- **Home:** This is the most relaxed security setting. Data can be sent unencrypted and other devices are free to access files from your device.
- **Work:** Common authentication and encryption systems are in place. Folders have to be shared. Most often Public key cryptography or Certificate Management is in use to protect the transfer of data.
- **Public:** The most secure. Here everything is blocked other than direct internet access, which is still managed tightly.

Think about it this way: You wouldn't leave your smartphone on a public bench. It may well get stolen.

Windows Firewall

←

→

⌵

⬆

⌵

⌵

⌵

⌵

⌵

⌵

⌵

⌵

⌵

⌵

⌵

⌵

<< System and...

> Windows Firewall

⌵

↺

Search Control Panel

🔍

Control Panel Home

Allow an app or feature through Windows Firewall

Change notification settings

Turn Windows Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

See also

Security and Maintenance

Network and Sharing Center

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks

Not connected

⌵

Guest or public networks

Connected

⬆

Networks in public places such as airports or coffee shops

Windows Firewall state:

On

Incoming connections:

Block all connections to apps that are not on the list of allowed apps

Active public networks:

🛋

Network 2

Notification state:

Notify me when Windows Firewall blocks a new app



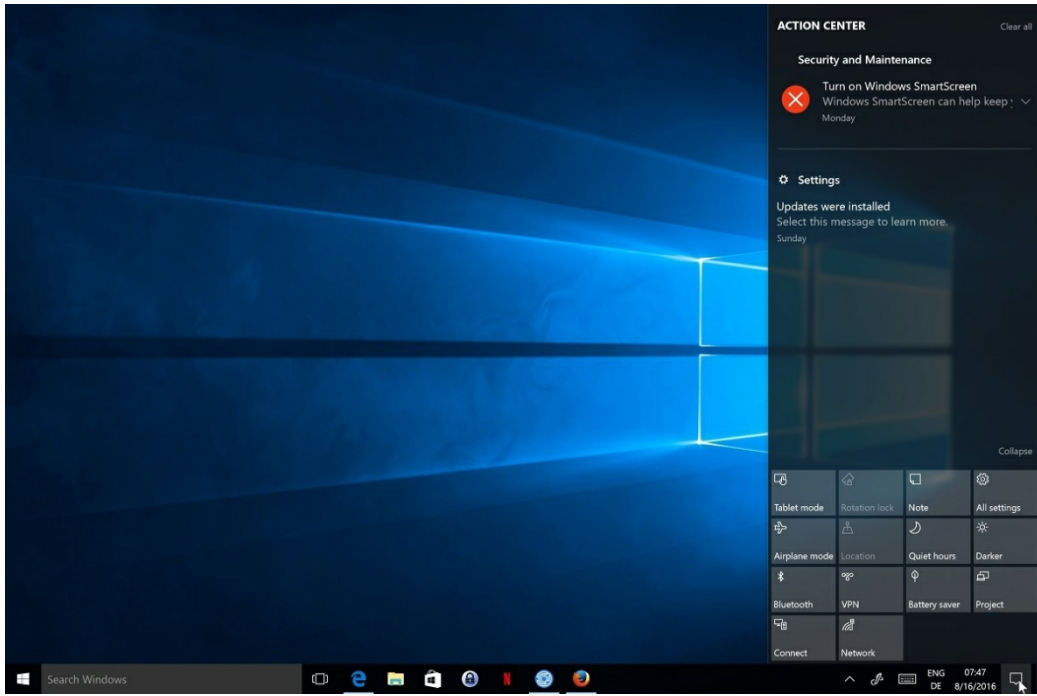
# Security Center

Security Center was first introduced with Windows XP to be a security dashboard. It was a traffic-light pane alerting the user if there was work needing to be done, or if one of the three key security tools were not enabled: Firewall, Windows Automatic Updates, and Malware protection.



It was set so that you would see a red shield on the taskbar if any of these were not switched on and was a way to train the user to be more security-conscious.

It was later branded as ACTION CENTER (where Microsoft corrects the spelling for UK users) and in fact does a lot more than people realize. The ACTION CENTER version can send system health data to Network Health Policy and Remediation Servers. These are used in the Enterprise environment and are very helpful in the situation where you have a member of staff who has worked away from the office for several months and may not have kept their system up to date, or 'clean'. When the user tries to connect to the office network they receive an IP address from the DHCP server as normal, but the IP number given is for a quarantine zone where there will be a remediation server, such as a **Windows Update Server (WSUS)** waiting for them. Only when scans have been run and Action Centre reports back with health data that conforms to the rules set on the Health Policy Server can the laptop retrieve a valid IP address.







# Event viewer

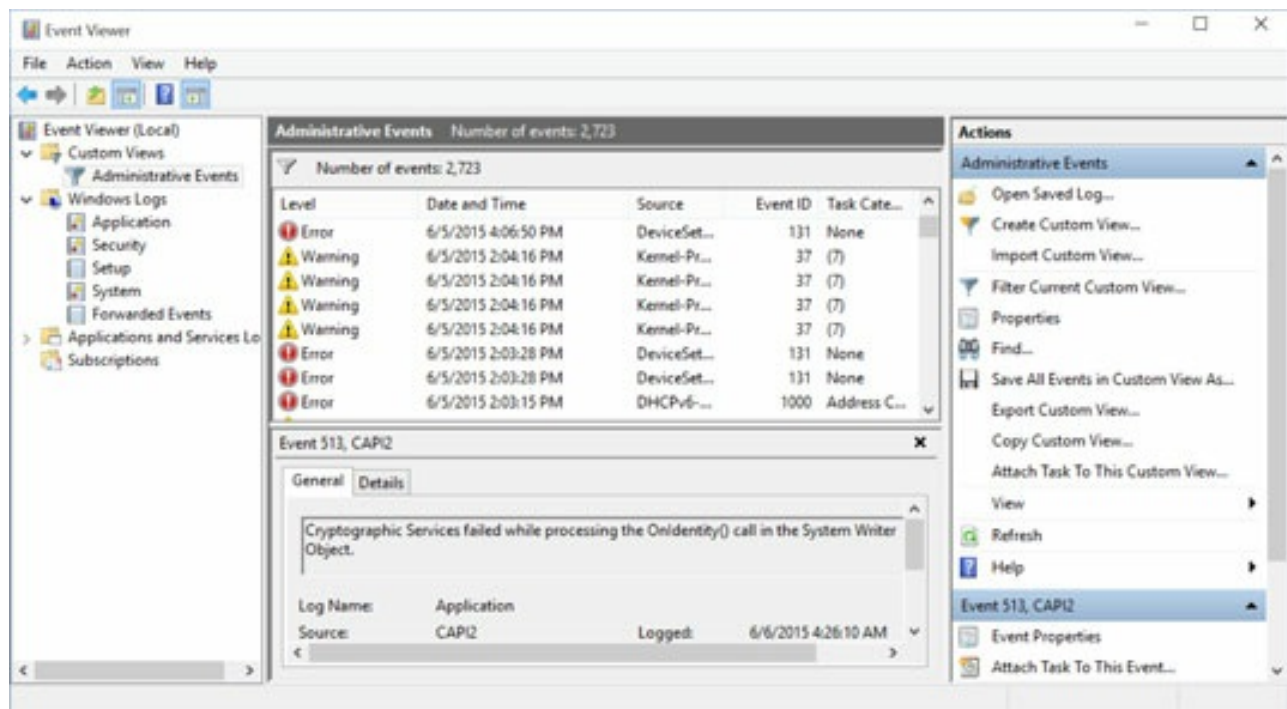
There are three significant logs the system saves event data to. These logs are of a set size and when full will start again from the start on a rolling structure. It is important that you therefore back up the logs and refer to them over time to check for problems that may not be as noticeable.

A good technician checks the logs regularly for errors and builds up a Red Book or knowledge database of common errors and fixes. Where possible they also create PowerShell scripts that could be batch processed to all affected machines across the network.

The three key logs are:

- System: This records any changes or problems with the modules that collectively we call the Operating System
- Application: This log refers to problems with non-system applications, for example, if Google Chrome hangs
- Security: This log records login attempts not only by the user, but for every app and service that runs against a service, user, or computer account

These logs grow to be quite large and it is common to record good actions as well as problems. You therefore will need to filter the log to pinpoint the exact problems you may want to resolve.



On a domain, logs can be sent from each client computer to a common PC, called an **event collector**. These logs can then be searched from this central PC making it not only physically easier for the Network Administrator to check the data, but more importantly it can audit the number of machines that have been affected as many may share the same problems.

Taking the analogy one stage further, maintenance software such as System Center or Intune can produce network-wide management reports detailing how many machines are affected, but cleverly it can roll-out a fix to all of the affected machines in one go.



# File structure and paths

The Windows file system is much easier to work with than Linux, which has a reserved area for the root user. The Operating System sees logical drives referred to as Volumes. Each are given a drive letter and the first available letter used is `C:`:

Why not use `A:` or `B:` ? This is historical. Early IBM x86 systems would have two floppy drives installed. One is to boot the core program (for example, PASCAL or DOS) and the other would be used to access your user data. These were drives `A:` and `B:`. Later x86 systems used one 3 1/2 inch floppy drive capable of storing 1.44 MB data, so the user data could be stored on the same disk as the core program, or the core program could be loaded into memory first and then the disk swapped over. In this case `B:` was redundant. DOS read the same floppy drive regardless of whether you used `A:` or `B:` as the volume.

When the operating system is installed the next available volume letter is used (`C:`). `D:` is usually also assigned at this point to the DVD-ROM. Any other volumes you may wish to create will then take the next available letter.

When the Operating System is installed, initially the hard drive is empty. Partitions are created (on the Windows system we only need one. Linux uses several). The partition start and end points are recorded on a table located at the start of the system disk. This is referred to as the MBR, although newer systems can use an alternative to MBR referred to as the **GUID Partition Table (GPT)**. This is a database of partitions.

There can only ever be one MBR/GPT table per disk. This is marked as active and the others on other disks are ignored.

If you have more than one hard drive installed and decide to install multiple operating systems it is possible that you may have more than one MBR/GPT available. The last operating system installed will have marked its GPT as the active GPT to use. However, things can get mixed up if the boot order is changed in the BIOS. Here, you might load a previous GPT located on another disk, so you will not get all of the installed OSes available to you.

The MBR/GPT essentially tells you where to find a file called the **Boot Configuration Database (BCD)**. This is a tiny database located at the front of the partition and lists where the actual installed Operating Systems can be located. What follows is an entry from a BCD showing multiple Operating Systems installed:

```

Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32>bcdedit
Windows Boot Manager
identifier {bootmgr}
device partition=\Device\HarddiskVolume2
path \EFI\Microsoft\Boot\bootmgfw.efi
description Windows Boot Manager
locale en-US
inherit {globalsettings}
default {current}
resumeobject {ffd3d3ae-17d1-11e5-9928-a30c6df423db}
displayorder {ffd3d3b7-17d1-11e5-9928-a30c6df423db}
{ffd3d3b3-17d1-11e5-9928-a30c6df423db}
{current}
{ffd3d38d-17d1-11e5-9928-a30c6df423db}
{f5776b47-c167-4b52-9edf-c73340c091f4}
{ffd3d3a2-17d1-11e5-9928-a30c6df423db}
toolsdisplayorder {memdiag}
timeout 30
Windows Boot Loader
identifier {ffd3d3b7-17d1-11e5-9928-a30c6df423db}
device partition=V:
path \Windows\system32\winload.efi
description Windows 7
locale en-US
inherit {bootloadersettings}
recoverysequence {ffd3d3b8-17d1-11e5-9928-a30c6df423db}
recoveryenabled Yes
osdevice partition=V:
systemroot \Windows
resumeobject {ffd3d3b6-17d1-11e5-9928-a30c6df423db}
nxOptIn
quietboot Yes
sos Yes
Windows Boot Loader
identifier {ffd3d3b3-17d1-11e5-9928-a30c6df423db}
device partition=S:
path \Windows\system32\winload.efi
description Windows Server 2012 R2
locale en-US
inherit {bootloadersettings}
recoverysequence {ffd3d3b4-17d1-11e5-9928-a30c6df423db}
recoveryenabled Yes
badmemoryaccess Yes
isolatedcontext Yes
allowedinmemorysettings0x15000075
osdevice partition=S:
systemroot \Windows
resumeobject {ffd3d3b2-17d1-11e5-9928-a30c6df423db}
nxOptOut
numproc 4
hypervisorlaunchtype Auto
quietboot Yes
usefirmwarepcisettings No
Windows Boot Loader
identifier {current}
device partition=C:
path \WINDOWS\system32\winload.efi
description Windows 10
locale en-GB
inherit {bootloadersettings}
recoverysequence {ffd3d3b0-17d1-11e5-9928-a30c6df423db}
recoveryenabled Yes
badmemoryaccess Yes
isolatedcontext Yes

```

```
allowedinmemorysettings0x15000075
osdevice partition=C:
systemroot \WINDOWS
resumeobject {ffd3d3ae-17d1-11e5-9928-a30c6df423db}
nxOptIn
numproc 4
bootmenupolicy Standard
hypervisorlaunchtype Auto
quietboot Yes
usefirmwarepcisettings No
```

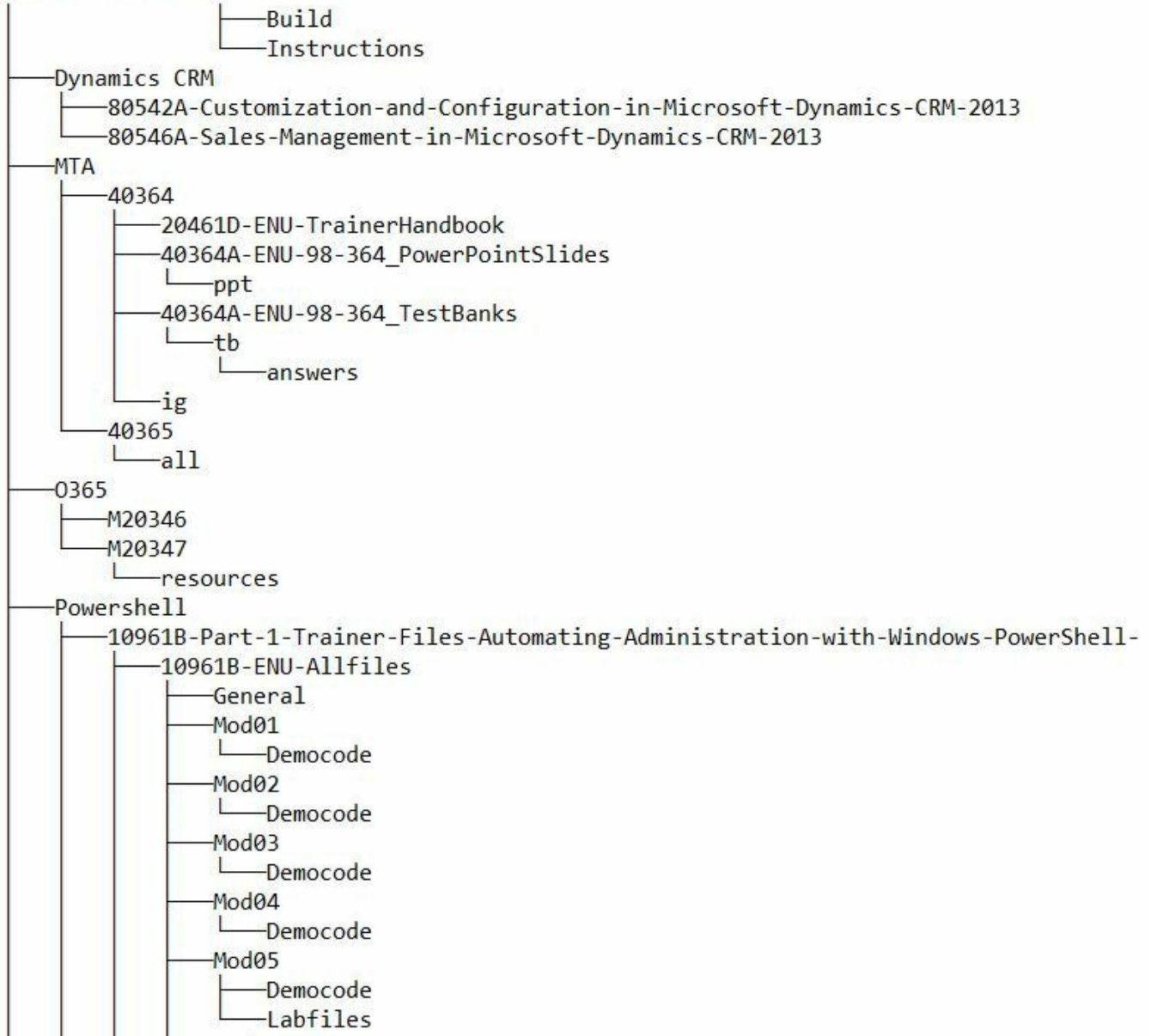
In this example, we see a boot manager and three possible operating systems and where they are located (Windows 10, Server 2012, and Windows 7).

As part of the install process a folder on the host volume (c:) called `Windows` is installed. Within the `system` and `system32` are the 64-bit and 32-bit (respectively) core system files.

It is also worth noting that any applications are installed into the `Program Files` folder. This is referred to as the `native` folder; 32-bit architecture will only have the one `Program Files` folder that stores the 32-bit applications. However, on a 64-bit architecture `Program Files` stores the 64-bit applications and `Program Files(x86)` stores the 32-bit applications.

Whilst we commonly use File Explorer, in a Command Prompt the following commands are used to navigate the folder structure:

- `CD`: List the current directory
- `CD <path>`: Change to directory
- `CD..`: Go up one level
- `CD\`: Go to the root of the volume
- `<drive letter>`: Change to another volume
- `MD`: Make a new directory
- `RD`: Remove a directory (needs to be empty first)
- `DEL`: Deletes a file from the directory
- `DELTREE`: Deletes a folder and its child folders
- `TREE`: Shows a graphical view of the folder tree







# Category view versus Classic view

There are three ways to display the icons within Control Panel.

Classic View lists all of the icons in alphabetical order. This is favored by technicians who know what they are looking for. The icons can be displayed in either Large or Small size.

Category view groups common icons by their use and purpose. Here, there is a two-tier approach. First, the section headline takes you to a customized page for the category listing all of the options available. There may well be more options that first appear by counting the number of icons underneath the category. Second, we have some of the featured icons related to that category (but not all of them).

Adjust your computer's settings

View by: Category ▼



## System and Security

Review your computer's status  
Save backup copies of your files with File History  
Back up and Restore (Windows 7)  
Find and fix problems



## Network and Internet

View network status and tasks  
Choose homegroup and sharing options



## Hardware and Sound

View devices and printers  
Add a device  
Adjust commonly used mobility settings



## Programs

Uninstall a program



## User Accounts

Change account type



## Appearance and Personalisation

Change the theme



## Clock, Language and Region

Add a language  
Change input methods  
Change date, time or number formats



## Ease of Access

Let Windows suggest settings  
Optimise visual display

For the exam, you will need to learn both view types and how to navigate the breadcrumb to get to specific panes. Notice that certain categories names have changed over time (Printers and Faxes becomes Devices and Printers, then Hardware and Sound).

From Windows 8 onwards there is now another control panel. This is designed to keep the end user away from the main control panel--a number of tablet and device functionality settings can be configured here and this acts as a buffer preventing the end user from immediately accessing the Control Panel. This can be accessed from the

Settings cog, from the Settings right pane (charm), or from the start menu on Windows 10.





# Side-by-side apps

This is a rather confusing topic as refers to two very different things. Side-by-side apps refer to Aero Snap, which is looked at earlier in this chapter. Here, we can open two apps and have them displayed on the screen side-by-side. The most common use is to move files from one location to another using drag and drop.

However, Windows uses a system folder called SxS (Side-by-side) to keep a copy of installation files, along with updates to these core files. Over time the SxS folder can become quite large (several GB), but it is worth noting that Windows is a self-repairing system and can use these files to reinstall any software currently available that may have become damaged and need to be repaired. Without SxS you would have to reinstall Windows from the installation media.



# Metro UI

We now call it the Start screen, but you will still see many articles referring to the Metro theme. For legal reasons we are no longer allowed to refer to this as such as Metro is a copyright protected brand and Microsoft lost the rights to use this name when referring to this product. (CompTIA refer to Metro UI in the exam objectives which is why it is used here.) The Start screen, as it is now known made its debut in Windows 8, but was criticized because most customers to this point were still on PCs, not tablets, or multi-operation devices such as the surface so the User Interface change was a big step for some. Windows 8.1 came with an option to boot to the Desktop, rather than the Start screen and then Windows 10 provided the more classic Desktop with an integrated Start Menu with live tiles.

The Start screen is designed with touch-sensitive devices (for example, tablets) in mind. Tiles can be grouped, resized, and moved. Live tiles show constantly updating data (for example, Weather or stock market live data), although most show an icon or game image.



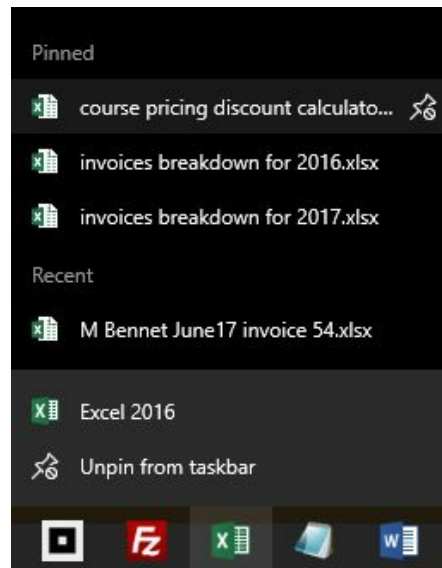


# Pinning

Apps that are used frequently can be easily accessed from either the Start screen or the taskbar. Once an application has been launched it will appear in the taskbar at the bottom of the screen. Right-click on the icon and from the jump-list you can pin it permanently to the taskbar.

One advantage of pinning applications that save files, such as Excel to the taskbar is that by right clicking the app in the taskbar you get a jump list containing previously pinned files and recent files that can be selected to be pinned as well. The Pinned section therefore contains files that can be opened using this app. For productivity reasons I have a pricing calculator Excel spreadsheet that I use regularly to determine prices for my estimates. This is pinned to my Excel icon.

So not only can we pin apps to the taskbar, or start menu, but both areas show recent files used. These files can also be pinned within the same icon.





# OneDrive

Microsoft has provided free access to a cloud-based storage area linked to your Microsoft Live account, so as well as accessing your Hotmail emails you can also save your files and access them from any computer.

One advantage of recent systems, especially from Windows 8 onwards is a feature called **User-Experience Virtualization (UE-V)**. UE-V means that I can log on to any PC or laptop, anywhere in the world with my Live account and get the same login experience - my color scheme and settings will be the same on the new PC as on my usual PC. If I save files to my OneDrive account these files will also be available to me.

OneDrive is not the only solution and requires that you have (at least) a free Microsoft Live account. Other providers are also available (for example, DropBox or Google Drive).

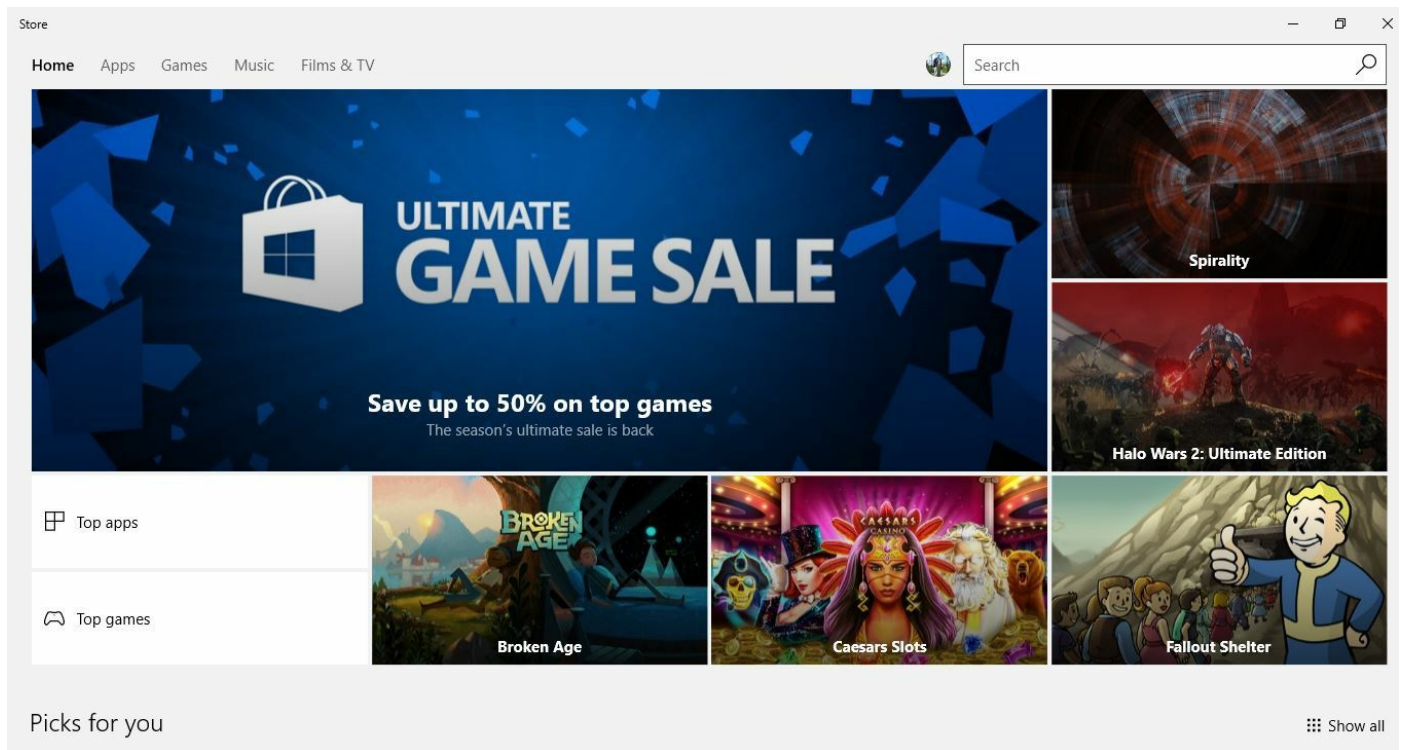
Note that OneDrive can also be accessed from the Desktop on Windows 8 systems or higher.



# Windows store

You will also need a Microsoft Live account to make purchases from the Windows Store. The Store, as with iTunes, or Google Play is a catalogue of publicly available apps, productivity features, and games.

The Store is accessed from the Play and Explore section of the Start menu as a Live Tile.



A business version of the store can also be set up--Windows 10 users connected to a domain may be restricted from accessing the public store, but instead can access a version of the store specifically designed for end users to access apps that have been specifically created for users to use at work. These apps are either public apps added to the business store, or apps created by the company for internal use.



# Multimonitor task bars

The Task View button is a new feature to Windows 8, but has been used extensively for years on Linux and Apple systems. The idea is that you can set up virtual monitors and each monitor contains a different set of icons. I might decide to put everything connected to productivity on monitor 1 and my games on monitor 2.

When only one physical monitor is in use Task View shows you the active apps and allows you to select an alternative live app to see, much as how Alt + Tab will do.

It is worth mentioning that each virtual monitor's taskbar will show the apps open on that monitor.





# Charms

A Charm is a screen edge pane available in Windows 8 and 8.1 (but removed from Windows 10) that shows the things you can do with the applications you currently have open. The Charm will therefore change depending on what you are doing, but the most common use is to access the Settings cog and from here to power down the PC.

The best analogy is if we compare the Android OS to the top settings menu. Here, you use a finger swipe down from the top of the screen to access the list of regularly used settings. A second swipe opens the full list of settings. On Windows 8, a swipe to the left from the extreme right of the screen will open the Charms bar that does much the same purpose.

On Windows 10 the Charms bar has been diminished and Action Center expanded to do much of the same functionality that we were describing previously.

The common five charms are:

- Search: A search bar appears but is limited to information on the screen. The scope can be expanded into a file search, or if you are on the Domain and Enterprise, or even a Federated search. Here, we can search the whole Domain, or even access material from the internet.

On Windows 8-10 systems you don't have to use the search at all. Press the Start key and even without the search bar present, simply ignore what is on the screen and type in the keyword you want to find. A search bar will automatically open with results scoped to app, file, or internet.

- Share: Where it is possible to share this information with someone else this will trigger an email to be auto-generated with a link of the page you are currently viewing added into the email already.
- Start: This is an alternative way to open the start screen.
- Devices: This allows you to output the existing screens' data to a phone, second screen, smartphone, or printer. In order for this to work correctly the second screen / device has to be installed first.
- Settings: This is the most useful as it enables you to get to the Windows Settings page. From here there is also a Power button where you can power down or restart the system.

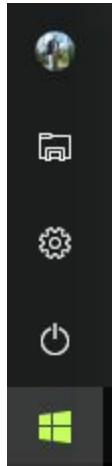




# Start screen

We mentioned the Start screen in depth earlier in this section. Windows 8 and 8.1 have a full-screen, tile-driven start screen that is customizable and great for use with tablets. However, it was unpopular with PC users who preferred the UI Desktop-driven interface, so Windows 10 is a compromise.

Note that on Windows 8, the active user is displayed at the top right of the Startscreen. From here you can log off, but you cannot power down from here. With Windows 10 the UI is more akin to Windows 7 in that the start menu is a menu again and a small Charms list appears just about the Start button containing the Settings cog, File Explorer, log-in icon (showing who has logged in. You can log off from here), and the power button.





# PowerShell

On Server 2012 by default Command Prompt has been replaced by PowerShell (Command Prompt is still separately available, but the normal shortcuts will take you to PowerShell). Client-side PowerShell is an extension and Command Prompt is still widely used. In truth, you can access a PowerShell session simply by typing `PowerShell` into the Command Prompt. The cursor will change indicating that a PS session is under way.

PowerShell is now a mature language. We are now using PowerShell v5 with backwards compatibility for earlier versions. It is based on the .Net code framework, so it will work with any apps created using .Net. All commands that could be done through the GUI, or a Command prompt can now be done with PowerShell equivalents. PowerShell is a Verb-Noun command language that is quick to learn and easy to use. There are only approximately four verbs available (for example, New, Get, and Set).

PowerShell also comes with a Scripting Tool known as **PowerShell ISE**. This allows me to create complex PowerShell scripts and save these for later use. I can automate processes and batch-process, affecting several computers at the same time with one script.

For the exam, you will be asked to read basic PowerShell code and work out the correct function to achieve the task. Learn Network equivalents for `IPCONFIG` and `PING`, also `NSLOOKUP` in PowerShell:

`IPCONFIG:` `Get-NetIPConfiguration`

`PING/PATHPING:` `Test-NetConnectionwww.microsoft.com -TraceRoute`

`NSLOOKUP:` `Resolve-DnsNamewww.microsoft.com`



# Live sign-in

A local account can be associated to a Windows Live account. On Windows 8 or higher go to Start | Settings and from the Windows Settings page select Accounts. Select the account you want to work with and here there is the option to associate a Microsoft account. This is not available from Control Panel | User Accounts on Windows 10.

Associating your Microsoft account means that you will add Federation information to your local account. Once you have signed in once, your credentials will be securely stored on the system allowing you access to all of the Microsoft pages, apps, and features you otherwise would have to sign into repeatedly.

This is most useful when switching from Windows Live (email) to OneDrive, or to Office 365. By using the online version of Office 365 you can save your work onto the OneDrive account, making it accessible from anywhere.

Network Managers may see this as a potential benefit because staff could work away from home. However, it is not managed by them when work is in a users' personal account, so it may give rise to corporate data theft. For this reason companies are often wary of cloud solutions they cannot directly manage. In this scenario the company might purchase a OneDrive for Business account and allow the user to use this business-focused Microsoft account instead of their personal one.





# Action Center

As mentioned earlier, Action Center (note the spelling) is now quite a useful tool. Originally, Security Center in Windows XP this showed us if the firewall was on and antivirus was working. We were given a traffic-light coded shield, showing us that the system was protected.

Behind the scenes and at Network level Action Centre reports to Network Health Validator servers whether the current security state meets the requirements needed to access the network. Until these are met the system cannot join the network.

Action Center has been developed over the years and now is en-par with Android's settings menu. It is designed to now replace the Charms bar to instead be a one-stop shop of buttons where the user can switch on or off functionality in much the same way as on a mobile phone. This is due in part to the fact that Windows 8 and higher is designed to work on a tablet and in fact the Surface is the hardware Microsoft had in mind. When the keyboard is docked it is a laptop. When the keyboard is undocked it is a tablet and should have the tablet-focused UI.



# Upgrading paths

There is a key distinction between updating and upgrading. Updating is the process of adding fixes, patches, service packs, and rollouts periodically through the life of the system making it more robust and secure, or adding new functionality. One of these recent rollouts available from Windows 7 and higher is in fact the new operating system: Windows 10. Upgrading from disc, or downloaded installation media can allow you to offline install by patching the existing files with the later version. This is known as an in-place upgrade. The alternative to this is wipe and load in which we completely replace the OS with the newer OS and re-add applications, drivers, and key data as well as migrating user profiles to the new system. This is used more if you want a clean system with no old files or unwanted configurations in the registry, also if you have had to refresh the hardware to support the newer OS.



# Differences between in place upgrades

An in-place upgrade is a messy solution and one that you as a technician should avoid. Here, you are upgrading the version of the Operating System, pasting newer files over the existing ones. The file structure remains intact and in terms of the amount of work needed this does not take as long as a complete rebuild (referred to as wipe and load). In-place upgrades are used when there is a version change but no need to significantly rebuild the system:

- Vista will not update directly to W10
- Windows 7 can upgrade directly to 10
- Windows 7 can upgrade to Windows 8
- Windows 8 will upgrade to Windows 8.1
- Windows 8 and Windows 8.1 will both upgrade to Windows 10

However, there are a few golden rules:

- You cannot downgrade editions (for example, you cannot go from Ultimate to Professional)
- You cannot change edition types (for example, Home is meant for small networks and home use, whereas Professional is meant for larger companies and domain use)
- You cannot change architectures (for example, a 64-bit OS needs to update to another 64-bit OS edition)
- You cannot change licensing types (for example, retail edition versus volume licensing)

Once the new OS is installed you have the option to trial the new system and roll back if you want to, but there is pressure on you as a technician to keep the system up to date. Vista and XP are now no longer supported and W7 will soon be phased out in the next few years. When the update took place a brand new Windows folder was created - rolling back will delete the new version and put the old files back into use. Once you are happy to stick with the new OS you can delete the old version using the Programs and Features list.



# Compatibility tools

We have already mentioned this in the 901 section of the book. If an app cannot run normally you can access the compatibility tab from the properties shortcut of the app in question. Here, you can set which version of Windows to emulate, if administrator approval is required for the app to run and also can reduce the graphics display settings as earlier apps may require to run at SVGA or lower resolutions.

Also available is the **Application Compatibility Toolkit (ACT)** that is part of the **Assessment and Deployment Kit (ADK)**. This is a suite of tools used for imaging and manipulating the current image, also tools for setting up unattended installations. Ultimately, this is used by second and third line support within a large company where you might want to deploy the same image to several PCs at the same time, or use Intune / System Center to build a PC based on how it will be used across the company. The ADK is available from: <https://developer.microsoft.com/en-us/windows/hardware/windows-assessment-deployment-kit>.





# Windows upgrade OS advisor

Built into the Windows 8 system is an app called Get Windows 10. This will appear in the taskbar on Windows 8/8.1 systems once the recent Service Pack has been installed (KB3035583). Alternatively, you will see an option to upgrade to Windows 10 in the Windows Update list.

Using the taskbar Get Windows 10 icon you can check the status of the existing system to determine if your present hardware will support the upgrade to Windows 10.

The process of upgrading takes approximately one hour. Core code will be updated, but otherwise the image remains intact.



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **An Overview of Windows Vista:** <http://www.professormesser.com/free-a-plus-training/220-902/an-overview-of-windows-vista-2/>
- **An Overview of Windows 7:** <http://www.professormesser.com/free-a-plus-training/220-902/an-overview-of-windows-7-2/>
- **An Overview of Windows 8 and 8.1:** <http://www.professormesser.com/free-a-plus-training/220-902/an-overview-of-windows-8-and-8-1/>
- **Windows Features:** <http://www.professormesser.com/free-a-plus-training/220-902/windows-features-2/>
- **Windows File Structures and Paths:** <http://www.professormesser.com/free-a-plus-training/220-902/windows-file-structures-and-paths-2/>
- **Windows 8 and 8.1 Features:** <http://www.professormesser.com/free-a-plus-training/220-902/windows-8-and-8-1-features/>
- **Windows Upgrade Paths:** <http://www.professormesser.com/free-a-plus-training/220-902/windows-upgrade-paths-2/>



## **902.1.2 Given a scenario, install Windows PC operating systems using appropriate methods**

In this next section we are going to look at the devices which can be used to boot into, the boot order and how we can partition and format drives for use comparing the uses and features of each.



# Boot methods

Contained within the BIOS is an important menu--based on the devices discovered what order should they be used to check to see if a bootable partition is present? Once the BCD or similar bootstrap files are located the OS will load, but it is just as easy to boot from a pen drive, or DVD. The boot menu determines the order in which these devices are checked for a bootable partition allowing the technician to add a repair DVD, overriding the existing hard drive and instead booting into the repair DVD to make key changes whilst the OS has not been loaded.





# USB

Within the BIOS you can set the boot order. Pen drives are commonly used to boot into an alternative system. As such they pose a massive security risk. For example, a person with a Linux distro stored on a pen drive could boot the system onto the stick and then retrieve files from the local hard drive. For this reason, incorporate environments you should never save files locally.

However, Microsoft have cleverly created a useful and positive spin on this issue. Windows To Go is a downloadable Windows 8/10 image that can be customized with corporate logos, apps, and drive mappings. More importantly, when the user loads the OS from the pen drive their local hard drive is locked and powered down. The computer boots from the USB stick and they cannot save any work other than to the stick, or to a mapped network drive. This is a good way to protect your data from theft.

The number of USB ports open can be set in the BIOS. It is common to have at least two back ports open to allow the keyboard and mouse, but then to close the rest unless you are planning to use Windows To Go to stop a user from trying to copy files onto their own local pen drive once the system has booted from the local hard drive.



# CD-ROM

As a technician it is good practice for you to carry a maintenance CD such as the **Windows Recovery Environment (Win RE)**. This is a set of command-line tools allows you to perform low-level maintenance such as to format disks, recover the MBR, or to recover the BCD. However, CDs are less common now.



# DVD

Most if not all modern systems require greater than 800MB on a disk. A typical OS install disk contains a series of images - for Microsoft systems you will find an Install.WIM file at approx4Gb in size containing the different editions of the operating system contained within the WIM as binary files. The installer files are heavily compressed and are copied into memory or onto a temporary storage location on the hard disk first. The system will amend the boot sector data writing an OS partition. The PC will restart and then instead boot from the hard drive from the extracted files. From here the system will perform a system audit and extract the files needed from the archive. The DVD is used only then to add on extra files not originally needed during the first phase of the install.



# PXE

It is now common for medium and large companies to be able to re-image a machine anywhere on the network. Retail outlets also tend to use dumb terminals (that is a PC with no hard drive installed) in public locations, such as in a shop front. A minimal OS is instead sent across the network from an imaging server and the stream can be multi-casted to several PCs at the same time.

The Pre-Execution Environment is a bootup option where the OS is installed into memory (for retail tills), or to the local hard drive (during a deployment). For this to work a few things need to be in place first:

- The PC NIC needs to be PXE-capable
- Any routers need to allow BOOTP traffic as the PXE communication is a series of Broadcast packets
- A DHCP server is required to provide an IP address to the PC before an image can be sent
- An imaging server is needed to host the image, also to stream the image to the waiting PCs



One of my best memories of working in IT was when I helped a friend of mine, a Network Manager at a local school. It was the summer break and the hall was still filled with tables as the summer GCSE exams had just been sat. We set up a server on the stage and connected approx.. 50 new PCs to the server. We started them and allowed them to boot into PXE mode. We sent out a multicast stream - the customized image, to all of the PCs at the same time. Within approximately three minutes I saw the Windows loading screen as all 50 PCs sprang to life.





# Solid state/flash drives

In many respects treat SSD as any normal mechanical hard drive. The main benefit of using SSDs is the extremely fast access times--data can be retrieved from an address block in a very short amount of time. There is no latency caused by 'spin-up' or the actuator arm moving to the correct position. There are also no concerns over damage to the platter; rather SSDs operate much like RAM.

It is important not to defragment SSDs. There is no need to do this because the time taken to retrieve the data from any block will be exactly the same, so it doesn't matter if the data is at the start or end of the disk.



# NetBoot

Apple systems can also PXE boot. NetBoot allows Macs with network-boot capable firmware to boot across the network. In relation to A+ see NetBoot as the Apple equivalent to PXE.



# External/hot swappable drive

Anything Hot Swappable means that the hardware can be safely removed whilst the PC is still powered without causing damage to the device, or causing the system to become unstable. An external drive often will connect through either a USB port or eSATA port.

Companies tend to run a rack (in the server room / Intermediate Distribution Frame) of powered, connected hard drives. These drives are visible to the OS. Using Windows Server you can create a Storage Pool, which is a collection of drives managed and controlled by the OS. We start by creating a list of drives the OS can work with. These are added to a group called the primordial. From the primordial we take as needed a disk drive and add it to the Storage Pool. The Storage Pool is a second grouping that is linked to a volume. The volume is often thin provisioned, meaning that we have said that we want a very large volume (for example, 100 GB), but from the outset no data has been stored. One disk from the primordial is taken out of this group and added to the Storage Pool. As data is stored it is saved to this one disk (which may be less than the overall size of the volume, for example, 1 Gb). Once this disk is filled another available disk is taken from the primordial and added to the storage pool, and so on. This allows us to create volume sizes much larger than the actual physical disk storage that we already have.



# Internal hard drive (partition)

In a disk categorized as a Basic Disk, the hard drive can be divided into four areas. The defining start and end points of these partitions are stored in the MBR / GPT table.

However, if the disk is converted into a Dynamic Disk responsibility for managing and recording these endpoints is given over to the OS managing the disk. A Dynamic SCSI driver is added to the bootstrap files to allow us to boot into the drive during startup.

Being a Dynamic Disk is also a requirement if we want to make use of RAID functionality (for example, Mirroring, Striping, Striping with Parity). Typically RAID 5 / 6 use a RAID controller card that gives quicker access times than the OS can on its own.

There should really be two physical internal drives --one for the OS partition and one for the data. This way you can back up your data without impacting on the OS, also take a system image backup of your OS, which will be reduced in size as it does not contain personal data.

Storage Spaces uses the concept of two (using three disks) or three-way mirroring (using five disks) as a backup option.





# Type of installations

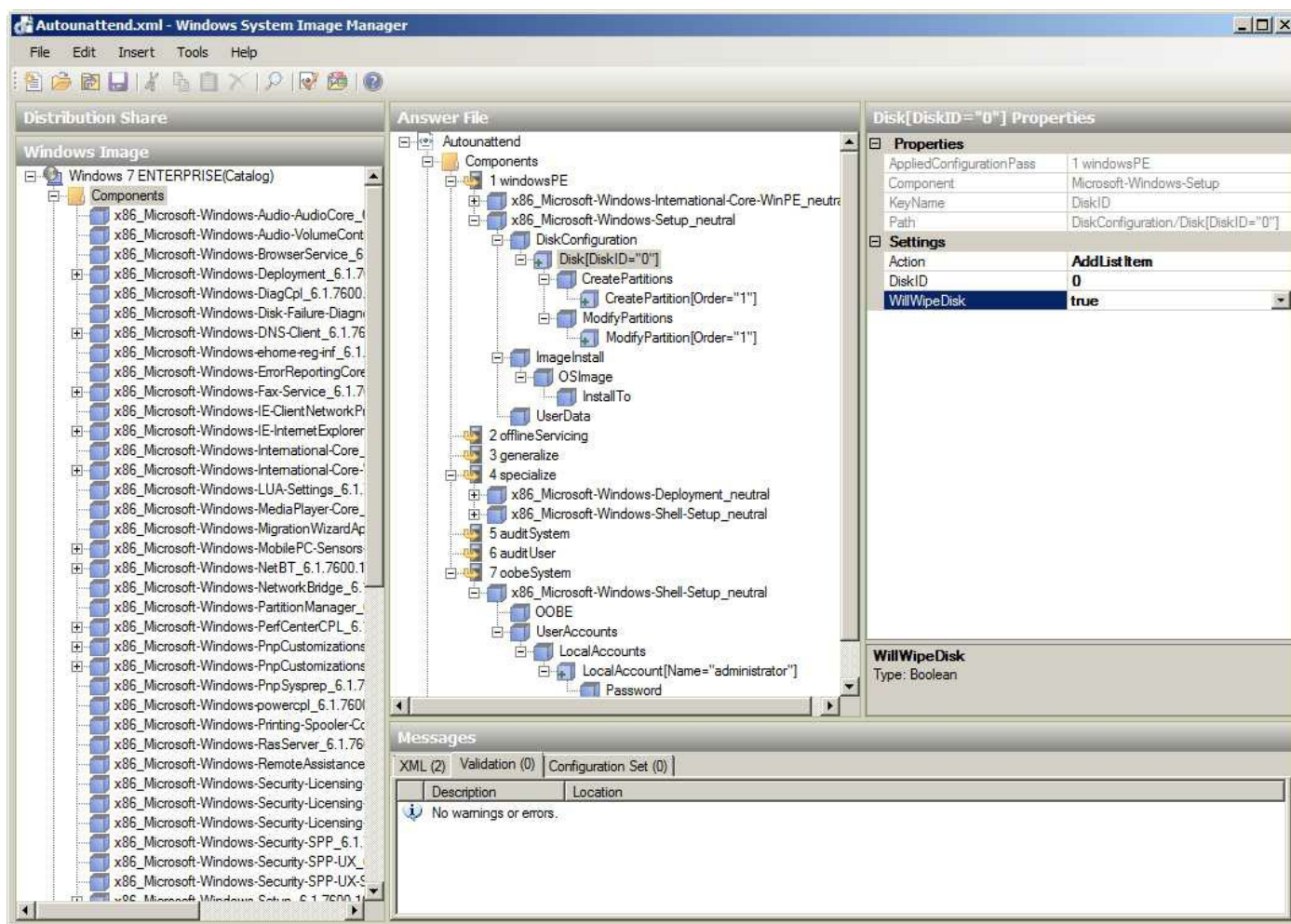
We have a variety of ways to install the OS from manual, light-touch (where some information is provided to the installer wizard but other settings still need to be set), or completely automated. Added to this a pre-baked image can be rolled out across the network to be installed on selected computers. When set up properly this can create an autonomous IT network that is self-healing.



# Unattended installation

Within the Microsoft Deployment Toolkit (available at: <https://technet.microsoft.com/en-gb/windows/dn475741.aspx>) is an app called the Windows System Image Manager. This is a clever application which allows you to add personal information, license keys, computer names, even join the domain as part of the install. In short, it creates an XML file (Unattend.xml) that can be used alongside the installation DVD to provide information automatically as it is needed. The XML file is either added to the same folder as the setup file on the install media, or is installed on a separate pen drive that is then read when the setup file is loaded.

By doing this you do not need to monitor or add information into the setup wizard as this information is already available. The installation will run as normal and take information stored in the XML file.







# Upgrade

The process of upgrading the OS typically will involve running the setup installation DVD from the existing OS. If it is upgradeable the setup file will load and realize that there is a host OS. As such, the existing OS registry and core files will be upgraded as an in-place upgrade.





# Clean install

A clean install adds the vanilla build of the system - core files from the installation media with no changes from the original system. It is therefore important that as soon as you are able to access the internet on this vanilla build, you should run a series of OS updates to patch the system to be most recent files.

The advantage of the clean install is that the footprint of the OS is smaller as it is not cluttered by legacy files, configurations, and drivers. Only the drivers required and found as part of the hardware scan as part of the installation process have been added, so there may still be a lot of work to be done afterwards to install other third-party drivers, software, and to perform configuration changes to the system to bring it back to the state it was in prior to the upgrade.



# Repairing installation

Here, we can repair the system without having to reformat and start all over again. By re-installing Windows from the install media and selecting the same folder as is currently used by the damaged OS, files are replaced with versions on the installation media, but the registry and configuration information are not replaced but tested and continue to be used.



# Multiboot

Different to an upgrade, booting from the install media bypasses any existing Windows version. Here, the installer files boot into memory. They do scan for existing Windows folders on the hard drive and if one is found you have the option to either update it or save the new version of Windows to a new partition if one exists. Here, the BCD is updated with a second entry for the new version of Windows and you now have the option to run the system as a dual boot PC, where you can access either the older OS or the newer OS.



# Remote network installation

Earlier on we discussed PXE booting and the requirements for this to work. An install image is sent to the PC typically in two stages:

- An IP address is assigned by the DHCP server on the network to the PC. This is issued by a sequence of DHCP commands (effectively a discussion between the two computers) referred to as the DORA process (Discover, Offer, Request, and Acknowledge). A minimal bootstrap is sent to the PC allowing network access, volume drive letters, and mapped drives. From here the image is accessible and can either be mounted manually using the Windows PE (Pre-installation Environment) if you have chosen to use this method. A Windows PE disk can also be used where the **Network Card (NIC)** is not PXE compliant and you have to provide the IP address and network mapping information a different way.
- The alternative, used with PXE compliant NICs is to retrieve a valid IP address and then to retrieve the main image in one go. This stream of data is several GB in size and may take 5-10 minutes or so to download. The stream can be multicasted to several PCs at the same time.

It is important to note (and we looked at this earlier) that what we are describing here is the roll-out of a pre-made image that will work on the target PC. All applications and configurations have already been set up so no further work needs to be done to the image other than to apply it, which happens the moment the image download is completed. This is applied by a simple restart.

It is worth mentioning a security feature built into Windows OS systems since XP known as System Preparation. When the OS is first installed a thorough hardware audit takes place and from this a `Security ID` number is generated. This SID will be unique to the PC - even if you tried to run the OS on a different PC of the same make and model it will not work. When you boot up the PC the OS performs a quick hardware audit and the same SID is generated. This is matched with the SID stored previously and the OS is happy to proceed. However, if the SIDs do not match something significant has altered in the hardware makeup of the PC to the extent where the change would occur, so it is possible the hard drive has been stolen from the original PC and placed into an alternative PC. As a result of this Windows Protection mechanisms will start and you will be prompted to reactivate your license. Failure to do so puts Windows into limp home mode (slows it down) and it will restart regularly until you relicense the machine. Images are generalized - they contain no SID. To do this, once the image has been

customized to the point where you are happy with it, run `SYSprep / GENERALIZE` to remove the `SID`, and then capture the image. On the target PC, once the image has been applied, run `SYSprep / SPECIALIZE` to make a new `SID`.

An image already pre-baked with a lot of existing software used across the company is referred to as a thick image. This is because it is a very large file with a lot of files contained within.





# Image deployment

The term imaging is used as a general term for the rollout of the data that forms the OS footprint. Deployment however refers to the process of building the OS remotely across the network, installing applications and OS features incrementally. Here a control PC (I use **Microsoft System Center Operations Manager, System Center Configuration Manager, and System Center Orchestrator**) identifies the blank PC by its MAC address, manages the issuing of an IP address through DHCP, can check Active Directory to see where this machine will be used (for example, it already has a managed computer object in an Organizational Unit) and from this knows which image to apply along with other later customizations to make and apps to install which are specific to where the PC will be used. The process of deployment involves creating a series of XML files and logic flowcharts to explain what, for example, a sales laptop would need to have installed onto it and the order in which changes are made to this PC. System Center sends both the installer files and also manages the process of sending the thin image to the target PC.



# Recovery partition

If you have bought an OEM PC it is highly likely that in the factory the hard drive would have a hidden partition installed that can only be accessed by a recovery disk provided by the OEM manufacturer. This recovery partition contained a heavily compressed archive containing the PC at the point it was when it left the factory. If you format your c: volume and do not have a Microsoft Windows Install disk then you will have to use the recovery partition to restore the PC back to the point it was when you bought the PC.

Any partition containing a system archive can be considered to be a recovery partition. These partitions are however usually hidden.

Be careful! If you are repairing an OEM PC for a client and format the disk you will lose the recovery partition. Most laptops have special drivers to access the hard drive and these drivers are also hidden within the OEM Recovery partition. The easiest way of removing the recovery partition by accident is to use a Microsoft Installation Disk rather than the OEM disk. Here, you will be prompted to format the drive and may well destroy the partition in the process.



# Refresh/restore

It is possible that either by deleting core system files, or after a virus attack (or other system damage such as corruption to the volume) the OS may not be bootable. The Microsoft system has an emergency Advanced Boot Options menu hidden and is accessible just after the POST test by pressing the f8 key. Here, one of the options is a Repair, which overwrites the core system files, pasting the ones from the installation media (or backup storage location such as the SxS folder) over the damaged files, restoring system functionality.



# Partitioning

The process of splitting the physical area of the hard disk into different areas is called partitioning. Using the analogy of the LP record, if you look at the grooves on the surface, you will see a dividing line where the recording is silent in between tracks. Consider this as similar to the partition points. With MBR the data is written as a table at the very end of the disk's available space. With GPT, a hidden partition is created and in fact various copies of the GPT database are stored across the disk.





# Dynamic

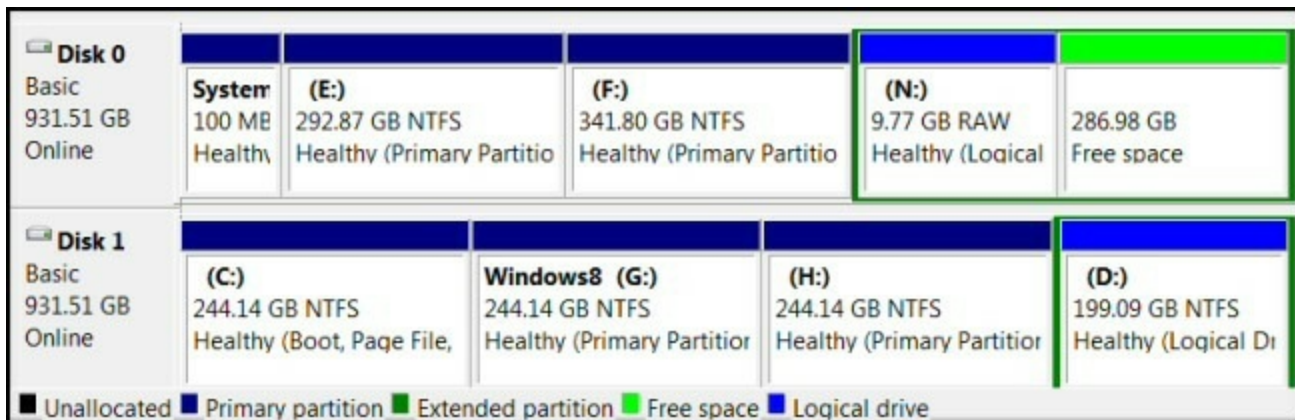
Dynamic disks are capable of so much more and are the preferred option when mounting and configuring a disk within the OS. Dynamic disks allow management information about what is stored on the disk to be managed by the OS and for this information to be updated on-the-fly, so you do not need to restart the PC for changes to take effect. Volumes can be made up of several partitions across several disks (spanning), or copies of the volume can be stored on separate disks (mirroring). RAID functionality (spanning, mirroring, fault tolerance) are therefore only possible where the OS is managing the disk set if the disks are set to Dynamic.



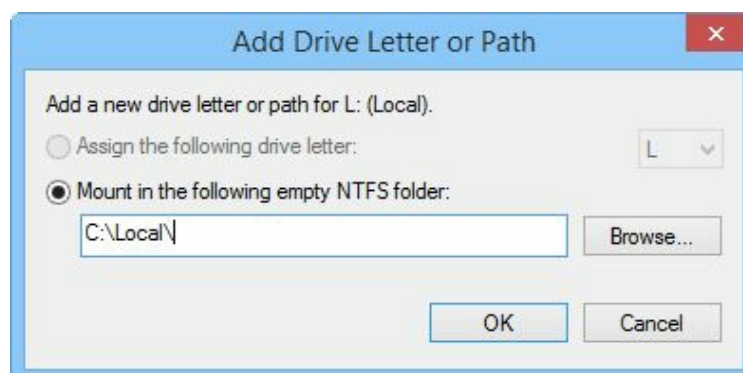
# Basic

A Basic disk is not capable of RAID functionality. Here we have only Primary or Extended partition, although if you need to create more partitions the Extended area can be split into Logical partitions that are controlled by the OS. These can be adapted and moved whilst the PC is live and no restart is required.

Basic disks are universal. If you ever need to dual boot and want to install a non-standard OS onto the PC then a Basic disk is the best option. It is good practice for the first disk on the PC (the one to be identified and to house the c: drive) to be a Basic Disk.



Given that there are limitations as to the amount of Primary partition you can create on a basic disk (four Primary, or three Primary + one Extended), we instead add Mount Points - that is an empty folder stored within the existing folder hierarchy that then gives you access to an area that has too much data to physically fit on the existing drive. Instead, the additional data (for example, a Music Library several TB in size) can reside as another disk and instead of accessing it through the volume letter, the mount point seamlessly integrates this extra data as if it were part of the existing drive:



- **Primary:** With a Basic Disk using MBR you are limited to four Primary partitions. Using GPT you can have 128 partitions. A Primary partition is a defined area assigned to a drive letter. There are limitations on the size of the partition and 2TB is a common limit for the size of a partition if you are using MBR.
- **Extended:** The Extended partition is an area you have given control over to the operating system. Within this space the OS can create as many Logical Partitions as it is able to, assigning mount points or volume drive letters as it needs to, shaping and moving the logical partitions however it needs to, but only within the Extended space.
- **Logical:** Within the Extended partition space the OS can create a series of Logical volumes. Each of these are independent and as far as the user is concerned operate the same way as any other partition. However, management and control of these is in fact provided by the OS and no data about the Logical partition is stored within the MBR, or GPT.
- **GPT:** GPT is synonymous with 64-bit architectures and is available from Vista upwards, but you need to be using UEFI rather than BIOS. As mentioned earlier, the GPT is a database containing information about where the partitions start and end. Each partition has a unique identifier as with a primary key on a database. The GPT database is stored in a hidden partition at several locations across the disk, not at the end of the disk as is the case with the MBR, therefore increasing the chances of still being able to access the GPT database. GPT is now also supported on Apple and Linux systems.



# File system types/formatting

Now that we have partitioned our drive and identified which areas, spanning disks if needed, make up our volume we can create a block structure to store the actual data. This process, known as formatting prepares the identified areas using a common system. Some formatting types are used with large volume sizes and are good for archiving and can self-remediate if the data should become corrupted. Other format types have additional security, encryption or compression mechanisms built-in and are widely used for this reason.





# exFAT

External FAT is an allocation table used on external devices such as SD cards and pen drives. It allows for files larger than 4 GB as other earlier systems would struggle to record a media file larger than this from memory to the storage device in one go. exFAT is the solution for this.



# FAT32

An improvement of FAT16, the FAT32 format is now universally used where OS systems are non-standard. Microsoft now recommends the NTFS system as the default when setting up a volume.

The FAT32 system is a 32-bit architecture. It was introduced in Windows 95 and Windows 2000 (in 2000) for corporate users. It was developed to overcome file size limitations. Cluster values are now represented by 32-bit numbering allowing up to 4GB as the maximum file size.

We use FAT wherever we need to guarantee compatibility with non-standard or non-Microsoft systems.



# NTFS

The NTFS is an advanced adaptation of FAT. It was introduced with Windows NT, in 1993 and has had many variants and upgrades over the years. It is considerably more resilient, self-healing to a large degree making it the more stable formatting system to use. NTFS also supports the use of encryption, compression (although not at the same time on the same file), and security properties. We can now set other users level of access to the file through a security list for the share and also a separate list governing the NTFS folder itself. By combining these two security lists and taking the most restrictive we can ensure that the file is secured.



# CDFS

The CD File System is an ISO recognized and universal formatting system specific to writing data to CDs and DVDs. It was originally invented for use on Linux, but is now widely supported. Each track stored on the CD is treated as a file and you can record both audio and data onto the same disc.

It was commonplace to have mixed media discs such as this with magazines in the 1990s, where an app would be on the first track, but skipped if played on a domestic CD player that could only read the audio tracks.





# NFS

The **Network File System (NFS)** was originally invented by Sun Microsystems in 1984. It is an open standard and therefore used widely. It governs the management of and sending of files across the network. On Microsoft systems we use **Server Message Block (SMB)** to manage the actual sending of files across the network. This defines which data the blocks are stored and then re-pieces the file back together where stored over several blocks.

File and folder navigation, mounting and dismounting drive letters, and other network functions are also performed by NFS.



# ext3, ext4

Breaking with tradition, but as we are discussing format types it would be good for completion purposes to mention the benefits of the Linux partition systems ext3 and ext4.

Ext3's main benefit is the introduction of journaling (documenting when files have been accessed and by whom). `ext4` allows for an easy and safe upgrade of the `ext3` filesystem, which provide storage and performance benefits when compared to ext3. Ext3 supports up to 16TB as the maximum file size, where Ext4 supports 1EB. Ext4 has an unlimited number of folders you can create where the limit with Ext3 was 32,000.

Ext4 is able to defragment as the volume is used (online), where Ext3 does not.

Sadly Ext4 volumes are not readable by Windows without third-party plugins and even then this is often in read-only mode.



# Quick format versus full format

When you format a drive, the quick format option does not scan the drive for bad sectors, where the full format will do this.

If you need to recheck the disk for bad sectors, use `CHKDSK /r`.



# Loading alternate third-party drivers when necessary

As identified previously, Microsoft's Windows platform is relatively universal, but cannot read ext3/ext4 partitions natively. Dynamic disks require the addition of the SCSI disk controller for that particular drive (the driver you will find in Device Manager for the physical disk drive) will be copied into the Bootstrap files as `Ntbootdd.sys`.

Normally we only load approved, digitally-signed drivers approved through Microsoft's approval program. Should you need to load unsigned or alternative drivers you will have to disable the enforcement of digitally-signed drivers (this is either a local security policy, or defined via a GPO on a domain). For 64-bit computers it is common to require digitally-signed drivers only. For 64-bit servers it is essential and is a safeguard built into the system.





# Workgroup versus domain setup

A network is a collection of devices able to share data and services between them. A network can exist in one of two logical forms:

- **A workgroup (peer-to-peer):** Here, each computer is set up independently and each machine manages its own services and own connections to other network resources.
- **A domain (client-server):** Here, common shared services are maintained by one device (centralized) and so wastage or duplication can be avoided. We will talk about a centralized network to refer to one specially designed PC that can perform additional services for other PCs on the network, even newly joined ones. This dedicated PC is referred to as the server. It is often made of more robust hardware, or has been scaled up to enable it to perform these additional duties.

Think about this from the perspective of backups - if I have 10 PCs and 10 users who constantly swap over which PC they are signing into then we have the potential of  $10 \times 10$ , which is 100 different user accounts. Each user account for each respective person would be different on a workgroup and each account stores different local user documents. You therefore have to back up potentially 100 user profiles.

For a domain, all user profiles are centralized and the same user profile is used no matter which client machine the user logs into. Therefore, there is only  $1 \times 10$ , so 10 user accounts to back up. The process is much simpler and these user accounts are stored on a centrally-managed file server.

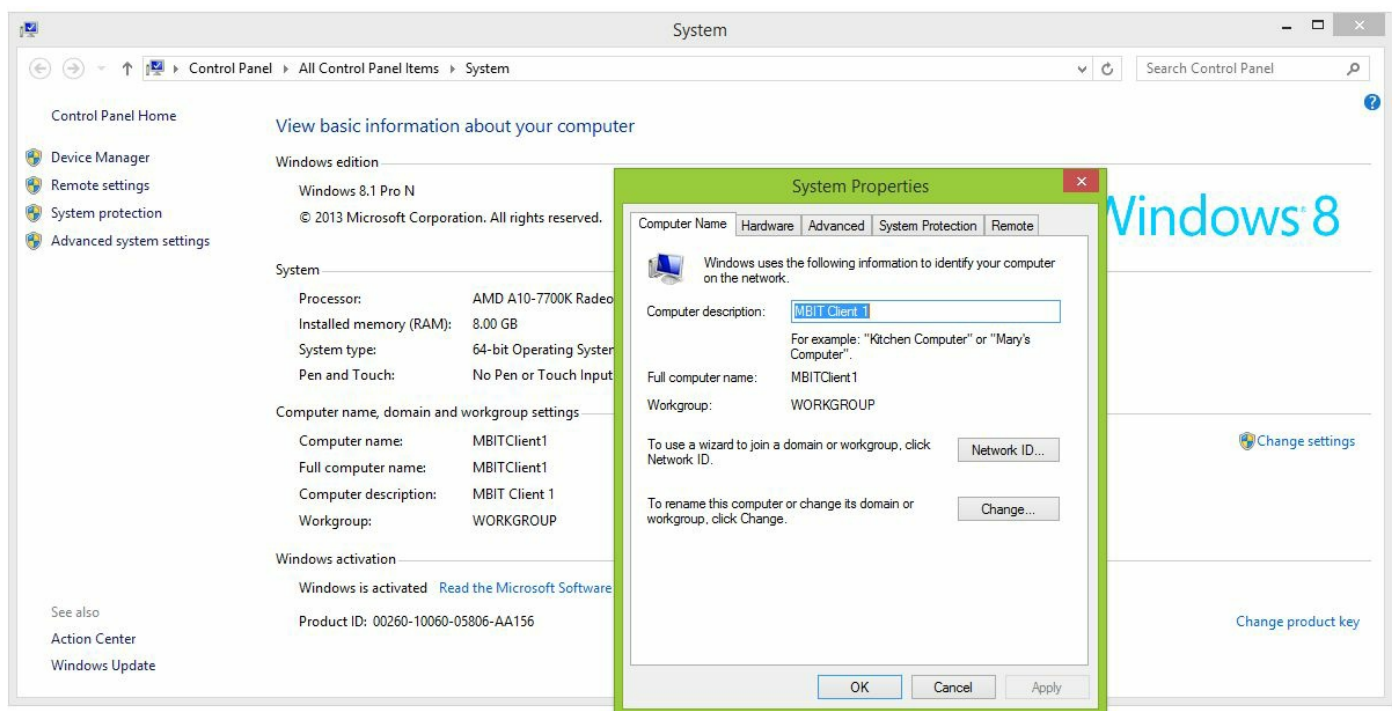
The Workgroup uses the local **Security Accounts Management (SAM)** database located on the local machine. Any shared resources have to be shared to that specific PC the client is using, so sharing can get quite messy. We use **NT LAN Management (NTLM)** for authentication, which is OK, but not as secure as a full Kerberos system. A domain has a secured database known as Active Directory in which our user and computer accounts are stored. When the user logs in they are presenting their credentials that are checked to see that they match the user and computer objects inside Active Directory. A challenge is created, made up of the details from the user and computer accounts, the username and the password. The answer to the challenge does not contain the password itself, rather is the answer once data from this security information has been passed through a special equation. The client challenges the server with its key information and at the same time the server challenges the client. Both challenges have

to pass. This is referred to as **MS-CHAPv2 (Challenge Handshake Authentication Protocol)**.

Once a machine has been installed it is a standalone PC. You can join a Workgroup by selecting the system pane from the control panel and pressing the Change settings link, which opens the Computer Name tab in System Properties where you can join a workgroup or domain.

For a workgroup, the PCs must be on the same subnet and have compatible IP addresses within the same range, have the same authentication systems, firewalls to accept Workgroup traffic, share the same workgroup join password (created when the original workgroup is made), and all use the same workgroup name.

For a domain, the PC must be contactable by the Domain Controller, have a valid IP address (it might be in another subnet, but this is OK), and when you connect to the domain you are using the Fully Qualified Domain Name (for example, Packt.com). For the DC to be reached you need an A (address) record in the DNS database for the DC to be found. To find DNS you need a scope options helper address in the DHCP scope, or have set the DNS IP one the client PC manually. When you try to join the domain you will need to authenticate with a domain administrator account at which point the computer object will be added into Active Directory.







# Time/date/region/language settings

To access this easily, simply click the time in the taskbar, at the bottom right of the desktop. From here you can use the change date and time settings link to open the date and time pane and set the correct time and date, also set daylight saving and time zone.

The language settings can also be changed in the taskbar next to the clock is a two-letter code (for example, EN) to determine the current language set in use. From here you can select an alternative display language.

If this does not show, you will need to customize the taskbar in which you can display this icon. Alternatively, you can access the language settings through Control Panel | Language.

Only install the language packs you actually need as these are quite large files and will waste space if not needed.



# Driver installation, software, and Windows updates

There are two different and important ways to install a driver through the GUI:

1. If the hardware is new, go to Control Panel | Hardware and Sound | Devices and Printers and select Add a device. This is the best option where the install may be complex, such as a three-in-one printer and scanner, or a web-camera that also hosts a built-in microphone.
2. If the hardware has already been installed and you are looking to update the driver, go to Control Panel | Device Manager, select the device from the hardware tree, and right-click. From the jump menu, select Update Driver Software, which will prompt to either run an automatic scan or give you the option to point to the location of the driver and information files if known.

Plug-and-play hardware such as USB devices have an ID chip built in that reports back what the hardware is to the OS, which then can install drivers supplied to Microsoft. This is often the best approach where you only want the driver to be installed and no other additional bloatware.

For printers it is good practice to install the driver and related software from the accompanying manufacturer's CD, or as a download from the manufacturer's website. Install it first and then only connect the device when prompted to do so as part of the installation. This is because some key drivers and low-level files need to be installed before the hardware can be discovered.





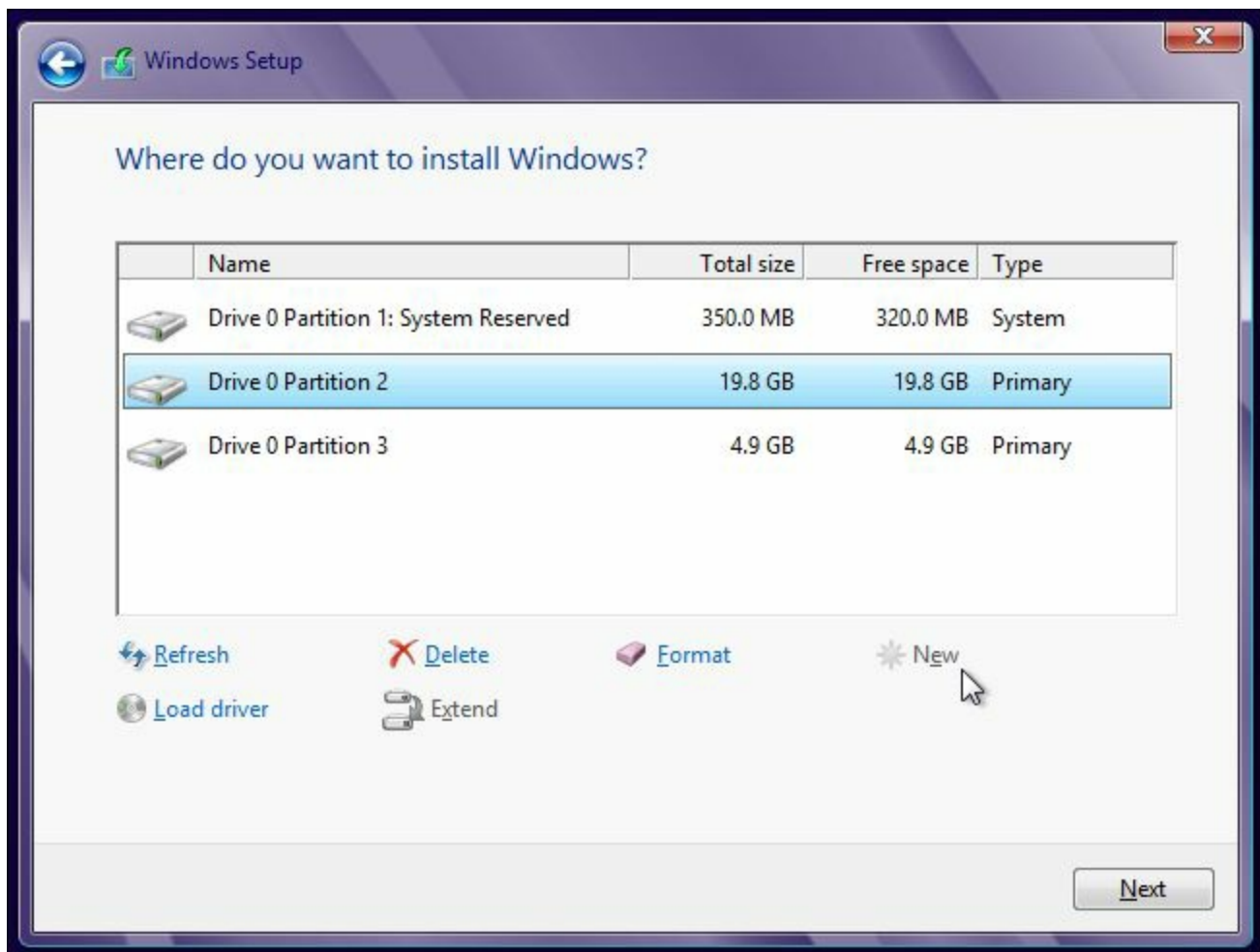
# Factory recovery partition

If you purchased an OEM PC you will have a slightly amended version of Windows that may not have all of the features installed, but may also have third-party software as part of the initial image. In the event of software corruption affecting the OS rendering the OS unbootable, there is a trick--a heavily compressed version of the OS image supplied by the manufacturer has been saved onto the hard drive. An escape key has been added to the BIOS (usually F1 or F11, but is different on each manufacturer - some supply a boot CD you have to use rather than an escape key), which will trigger a built-in process where the active partition will be wiped and replaced with the image as it was when it left the factory.



# Properly formatted boot drive with the correct partitions/format

If you use an original Microsoft Windows installer DVD on an OEM-build, there is a high probability that you may unknowingly wipe the OEM recovery partition. When you boot from the Windows DVD the installer will be loaded into memory and then you will have full and unfettered access to the hard drive where you will be able to create partitions as you require. If you choose not to set partitions, or wipe any existing ones then Windows, as it needs one anyway will create one primary partition the size of the entire disk and then format this as an NTFS partition for use.





# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Planning a Windows Installation:** <http://www.professormesser.com/free-a-plus-training/220-902/planning-a-windows-installation-3/>
- **Installing Windows Vista:** <http://www.professormesser.com/free-a-plus-training/220-902/installing-windows-vista-3/>
- **Installing Windows 7:** <http://www.professormesser.com/free-a-plus-training/220-902/installing-windows-7-3/>
- **\* Installing Windows 8 and 8.1 :** <http://www.professormesser.com/free-a-plus-training/220-902/installing-windows-8-and-8-1/>



## 902.1.3 Given a scenario, apply appropriate Microsoft command-line tools

Windows also contains an array of legacy, but still very useful command-line tools. Most of these are UNIX variants from the days of DOS, but are still in use. Please note that the preferred CLI commands are PowerShell equivalent commands; however, the following are still supported:

- **TASKKILL:** This is designed to end a currently running task that may be refusing to quit. For example, `taskkill /ssrvmain /f /imnotepad.exe` will close Notepad on a computer on the network called `SrvMain`.  
`/f` denotes that it will be forcibly terminated, so if there is anything within the programming structure stopping it to be unloaded (for example, the program is waiting on user input but the user cannot see the question in a pop-up window). `/im` is used to denote the image name of the app to close.
- **BOOTREC :** This can be found within the Windows Recovery Environment and is used to automatically scan and fix problems stopping the OS from being found during initial bootup. If the active partition cannot be found due to damage to the MBR, use the switch `/FixMBR`. On a dual-booting PC, in the event of an earlier version of Windows was installed on top of a later one, Bootstrap files will have been altered and are now unreadable by the newer OS. `/FixBoot` will fix this (you need to be in the Recovery Environment for the newer OS). `/ScanOS` is used where an Operating System is installed but missing on the BCD. Any entries not currently on the BCD store will be listed. If the BCD is damaged and unreadable `/RebuildBCD` will rescan all disks and their partitions and create a brand new BCD.
- **SHUTDOWN:** The `SHUTDOWN` command is used to send a shut down instruction to the PC. With the `/m` switch you can shut down other PCs on the network. With the `/t` switch you can set the delay before the actual command will action. An alert will instead be given to the other PC and the other user will have a few seconds to pass a `SHUTDOWN /a` (abort) command. `/s` completely shuts down the PC where `/r` forces a restart and `/l` logs off the user only. For example, `SHUTDOWN /s /t 0` will shut down the current PC immediately.
- **TASKLIST:** Using the same switch semantics as `TASKKILL`, `TASKLIST` shows a list of running processes (as with Task Manager), on the CLI listing their PID and memory usage.

- **MD:** Short for **Make Directory**. This is used to create a new folder in the existing location.
- **RD:** Short for **Remove Directory**. This is used to delete a created folder from the existing location, but this will only work if the folder is empty of files first.



On Microsoft systems the term Directory and Folder mean the same thing.

- **CD:** Short for **Change to Directory**. This is used to move the location pointer to a different path. By typing `CD <foldername>` you can navigate the pointer into a child folder 1 or x levels down from your current relative position. By using a full path (for example, `CD c:\temp\tempstore2`) you will jump directly into `tempstore2` irrespective of where you are. If your pointer is in a completely different location on the `c:` drive you will go straight to this child folder. `CD..` will take you up one level within the relative path (for example, from `tempstore2` to `temp`) and `CD\` will take you to the top-level of the volume (the Root location, for example, `c:\`).
- **DEL:** Short for **Delete file**. On some systems this can be used to delete files from the existing folder or from its children where a folder name is supplied. For example, I have a test folder called `c:\test` containing a child folder called `rd` that has a file present called `test.txt`. If my pointer is in the test folder and I type `DEL rd` then I will be prompted to delete all files inside of the `rd` folder, leaving the folder empty. For Windows 8 and 10, `DEL` will not delete the `rd` folder.
- **FORMAT:** Once you have partitioned a portion of your hard drive and assigned a volume letter to it, you need to structure how data should be stored inside of this region by creating a series of data blocks. These blocks are all set to the same data size and use the same physical space on the disk. As the disk is circular, tracks and sectors are created segmenting the area like a spider's web. Each block is typically 4KB in size. We can set the format of a volume to be FAT, NTFS, ex-FAT, or REFS. For CD and DVDs, the CDFS system is used.
- **COPY:** The `COPY` command is designed to be a simple copy action, copying a file, or series of files from one location to another. Please refer to Technet for full details of the switches available; however, common file copies do not require the use of switches, only two paths (the source and the destination) <https://technet.microsoft.com/en-gb/library/bb490886.aspx>.

As `COPY` is part of the DOS command interpreter, it can also allow us to write to the screen, or to directly print to a printer. It can concatenate the contents of files together, rather than simply copy a file from one place to another.



- **XCOPY:** This is actually a third-party command and therefore might not be available on all recovery disks, or versions of DOS. **XCOPY** is specifically used when copying files, folders, or entire directory structures from one place, or volume to another. With **XCOPY** the date and timestamp can be preserved.



For a list of related switches please visit at <https://support.microsoft.com/en-gb/help/240268/copy,-xcopy,-and-move-overwrite-functionality-changes-in-windows>.

- **ROBOCOPY:** Sometimes the connection between machines may drop in which case an **XCOPY** may fail. When copying a lot of small files (for example, taking a backup of a website) you need to ensure that not only is the copy of the file present, but also correct. **ROBOCOPY**'s advantage is that it will continue to retry until all of the files have been transferred, for the entire batch, which is why it is referred to as the Robust File Copy. Security permissions on the files are unaltered, so the copied data will be an exact image--this is useful when copying virtual machine files from one volume to another.
- **DISKPART:** This invaluable and powerful tool does everything you can do within Disk Management, but also sets partitions as the active partition. With this I can assign drive letters, create, resize and delete partitions and volumes, create RAID arrays, set a partition to be hidden or seen, mount, and join and break dynamic disks (where the dynamic disk is made up of several joined files, such as VHD files). **DISKPART** can be used also to alter the disk volume information storage from MBR to GPT and vice versa.



For a full list of features and switches refer to [https://technet.microsoft.com/en-us/library/cc766465\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc766465(v=ws.10).aspx).

- **SFC:** The **System File Checker** is used when you suspect that a core OS system file is either damaged or missing. The OS will perform a full scan of the Windows folder and its subsets and copy over from the install media (or the **winSxS** folder) replacing any corrupt or absent files. This is an automated process and is used with the **/SCANNOW** switch to perform a local scan.
- **CHKDSK:** **Check Disk** is used to check for physical damage to the integrity of a physical hard disk. With the **/r** switch we can also attempt to not only mark bad sectors as 'bad' and therefore unusable, but will try to recover data from these blocks and place them in known good blocks with free space. **CHKDSK** also checks the volume information and integrity, ensuring that there are no rogue entries and that

all folders present can be accessed.

- **GPUPDATE:** This is a particularly useful command when dealing with Group Policy settings. Typically the Domain Controller will send out Group Policy updates and new rules every 10 minutes, so in many respects this command is superfluous. It is run on a client computer if you want the new policy to be put into force immediately, rather than waiting for the update to be rolled out. If the GPO is a computer policy a restart of the client PC is required before the policy is enforced as new policies are read only during the OS boot process. However, if the GPO is a user policy the policy is enacted either immediately after running a `/Force`, or after logging off and then logging back in again as User GPOs are applied during login.
- **GPRESULT:** If a user has several policies applying to them at different scoping levels (for example, some are Domain-level, some are Site-level, and some are at OU level) then the Local policies apply first, followed by Site, then Domain, then OU. One policy may overwrite another. With Loopback processing and the fact that the user is also a member of groups it can soon get very complicated as to which and the extent to which the policy will apply and what the ultimate result for the user will be. On the Domain Controller the Group Policy Modeling Wizard found within Group Policy Management can be used to run a simulation and report detailing the eventual outcome for a specific Computer or User account. Client-side `GPRESULT` is the Command-line equivalent displaying a list of policies and which ones will affect the specific account.



There are several switches here, please refer to Technet as a guide:[https://technet.microsoft.com/en-us/library/cc733160\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc733160(v=ws.11).aspx).

- **DIR:** Short for **directory listing**. `DIR` allows you to see the files and folders present at the current level, relative to the pointer. If I am in a folder called `C:\Windows` I will see all files within this folder and also notice its child folders. I can see the filenames and creation and modification of timestamps and file sizes.
- **EXIT:** This closes the console window. If you are within another CLI tool such as `NSLOOKUP`, `POWERSHELL`, or `TELNET` this closes the session returning you to the DOS prompt with a pointer showing the current location.
- **HELP:** On its own `HELP` will provide you with a basic menu of all of the commands built into the DOS Command Interpreter. With `HELP <tool>` help information, switches and examples explaining what the tool is and how to use it is already present. There is no need to perform an online search (for example, Technet page) unless you need more detailed information.
- **EXPAND:** This is used to expand files out which have been compressed. Typical usage

would be to extract a folder and file structure from an archive file, or ZIP file. Third-party GUI equivalents would be 7-ZIP, Winzip, or Windows' own extract files feature.

- `[command name] /? - HELP` only provides information about tools that are part of the interpreter. Other third-party or additional commands have their own built-in help information page that can be accessed with the `/?` switch (which means that you do not know which switch to use so need further information regarding the switches available).
- Commands available with standard privileges versus administrative privileges - Many system features have safeguards built in to safeguard against accidental deletion, or other manipulation of the OS that could be damaging. Only a limited number of OS CLI and PowerShell commands can run in a standard user environment. If you need unfettered access we elevate (escalate) the privilege level of the Command / PowerShell window by using the Run As... option and specifying an Administrator-level account.



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Operating System Command Line Tools:** <http://www.professormesser.com/free-a-plus-training/220-902/operating-system-command-line-tools-2/>
- **The Windows Recovery Environment Command Prompt:** <http://www.professormesser.com/free-a-plus-training/220-902/the-windows-recovery-environment-command-prompt/>



## **902.1.4 Given a scenario, use appropriate Microsoft operating system features and tools**

This section will cover all of the key administrative tools used to control and configure aspects of the system. We will first look at key GUI tools and then a close consideration of essential tools that need further examination.





# Administrative

The Administrative tools are all of the GUI tools defined as needing Administrative privileges to be able to make changes to the system. Users have limited access to some of these, or read-only access that does not allow them to make changes to the existing system.

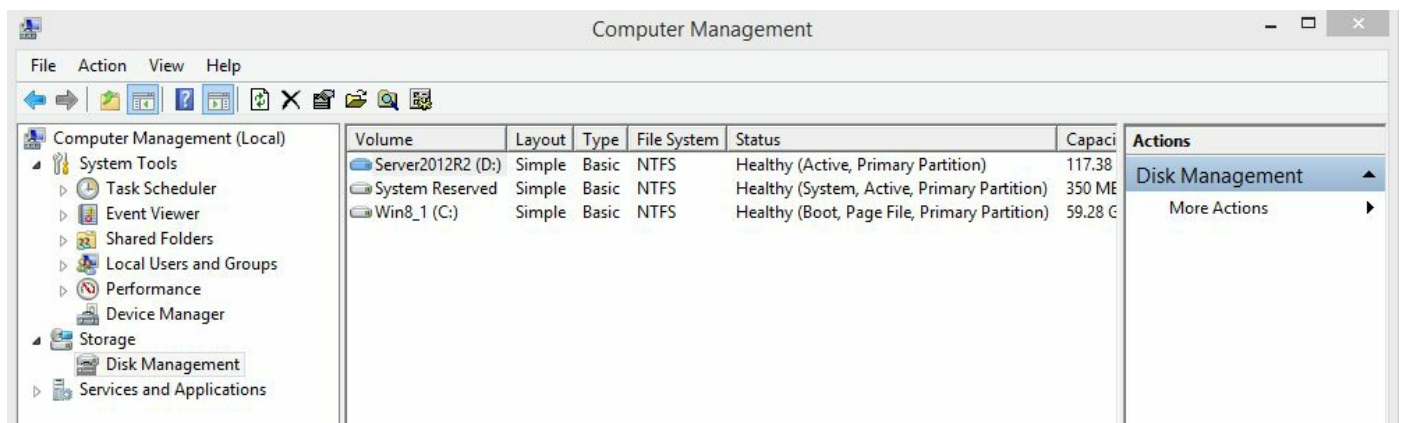


# Computer management

The Computer Management console is really not what it seems! It in actual fact is the **Microsoft Management Console (MMC)**--a blank window into which you can add snap-ins, that is, GUI tools and then save your selection as an MMC profile. This Swiss-Army Knife is invaluable to a technician as you can save the tools onto a USB pen drive and load them onto the computer you are working on.

Better than that, the MMC window allows you to not only open the tools against the local PC, but also ANY other computer on the network, presuming that Remote Management Tools has been installed on your client computers (you should, you really should!)

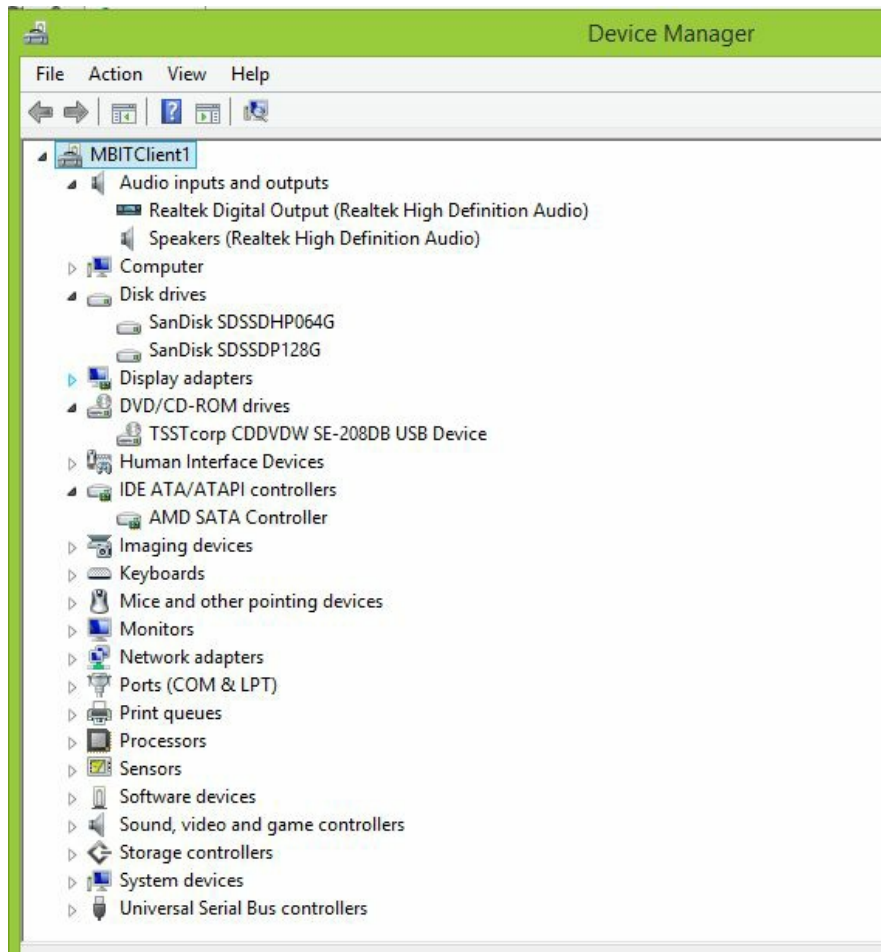
Computer Management is a pre-built MMC with a list of common tools used by most technicians giving you quick access to most of the common tools. It is accessible from the Start Menu jump list, also from Control Panel | Administrative Tools.





# Device manager

It is absolutely critical that you know how to get to and use Device Manager. Located in Control Panel and also on the Start Menu jump list, this is a family tree of all of the actual hardware components that make up your system. It also shows if a device is disabled (Down black arrow), or in a problem state (yellow exclamation mark).



As well as this right-clicking on a component you can access its properties, update its driver, or reconfigure it (for example, a Wi-Fi NIC may need to be set to the correct mode and duplex speed). Each device needs an **Interrupt Request (IRQ)** number and a **Direct Memory Access (DMA)** number.



# Local users and groups

This is very important for individual PCs not joined to a Domain - the Local Users and Groups tools shows all of the local user accounts listed on the SAM database. Within here you will find the Local Administrator account created when Windows was installed, used for maintenance on the local PC, a Guest account, and other local accounts you have for the PC.

There are also a series of built-in groups that are used to determine the extent a user account can access the system:

- **Access Control Assistance Operators:** These users query attributes on a file and security permissions, but not set them.
- **Administrators:** The group of people with unfettered and complete access.
- **Backup Operators:** Only people in this group can run a backup job, or restore from a backup.
- **Cryptographic Operators:** Only these people can edit, use, or create a certificate.
- **Distributed COM Users:** Only this group can launch COM objects on the system.
- **Event Log Readers:** Only this group can read the event logs.
- **Guests:** These have the same access rights as the standard users in the Members group. There are slightly tighter restrictions, but the fact that the person is not named in the Event Log is enough to justify that you should never use the Guest account as you do now know the real identity of the person accessing your network. It is more preferable to add a specific account for the guest with their actual name and then lock it down by adding it to an Organizational Unit.
- **Hyper-V Administrators:** Only people in this group can create Virtual Machines, delete them, or reconfigure them.
- **IIS-IUSRS:** The IIS (Web Hosting) service uses this group to identify users who can access IIS websites.
- **Network Configuration Operators:** These can make changes to IP addresses assigned to network devices.
- **Performance Log Users:** These users can start logging specific logs.
- **Performance Monitor Users:** Once created, these users can read performance counters that have been previously saved. This applies to the local system and also other PCs on the network.
- **Power Users:** A half-way house between a standard user and an Administrator, this level has limited access to higher functions on the PC.

- **Remote Desktop Users:** These users can log on remotely and use the Remote Desktop App.
- **Remote Management Users:** Only these users can issue Remote Management commands, such as PowerShell commands issued against other PCs.
- **Replicator:** These users can copy files across the Domain.
- **Users:** This is the typical User group where standard users are stored.
- **HomeUsers:** These users are part of the HomeUsers security group.
- **WinRMRemoteWMIUsers:** These users can use the Windows Management Instrumentation protocol to determine if a PC is of a certain type of hardware, or OS (for example, laptop running Windows 8.1) and use this information to determine if a policy should be applied.





# Local security policy

There is a local and stripped-down version of Active Directory's ADO database. Local policies are applied first and normally when the PC first boots up. If the PC is part of a domain other domain-level policies afterwards and may override these, but it is important that you lock down the PC as much as possible locally, first.



# Performance monitor

The performance monitor is a graph capable of showing real-time live data, and it can also be used to replay binary data captured previously. There are several hundred counters you can select to look at different aspects of the system covering processor, memory, NIC performance, hard drive speed, and so on. As other software is installed, for example SQL Server, additional counters are also added. Output can be either by a real-time updating report or graph.

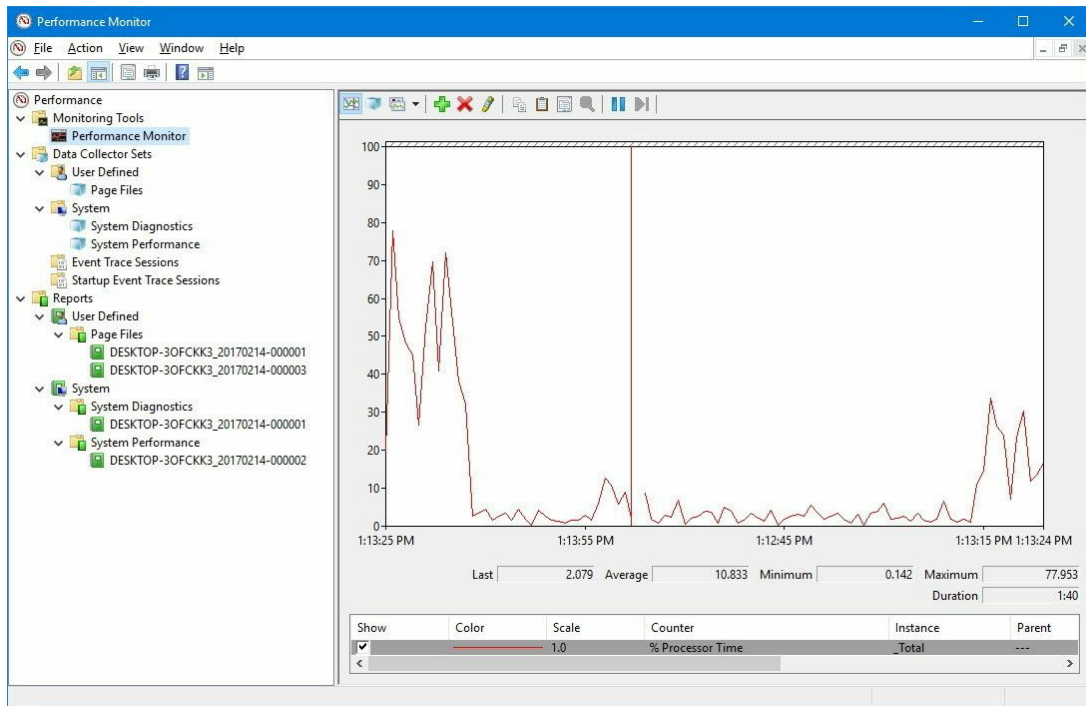
One issue with Performance Monitor is that it is common to see multiple counters be used on the same graph, but have different scales on the y axis, so you need to determine what good looks like.

The best way of using the Performance Monitor tool is once an approved image has been taken on a reference computer. Capturing data of the system at its best state will give performance data you can use as a baseline (benchmark) and can compare changes from this to see if the system has improved or degraded over time, which in turn can direct your configuration actions.

Key counters to know are:

- **% Processor Time:** This gives an overall activity of processor use. A constantly high value would indicate that the system is over-taxed and would benefit by a faster processor, or more cores.
- **Current disk queue length:** This tells you how many files are queued to be written to the disk. A number greater than two or three would indicate that the disk is too slow for the system.
- **Page reads/sec:** This tells you the access speed for the RAM. A small number would indicate slow RAM.
- **NIC Current bandwidth:** This gives the current bandwidth in Mb/s of the NIC. If it is lower than you expected there may be an issue with the connection to the switch, or the TCP/IP stack is being very tentative and starting your connection on a file transfer too slowly, or the number of connections allowed may be misaligned.

Each counter can be focused to look at a specific hardware component (for example, only one drive), or report back on all of them.



Computer Management also features the Performance Monitor. Performance Monitor requires that you create a collection of counters and store this data as a Data Collector Set. Using the collector set allows you to take typical performance readings and produce a report showing the current performance of the system.

Computer Management

File Action View Help

Computer Management (Local)

- System Tools
  - Task Scheduler
  - Event Viewer
  - Shared Folders
  - Local Users and Groups
- Performance
  - Monitoring Tools
    - Performance Monitor
  - Data Collector Sets
    - User Defined
      - New Data Collector Set
    - System
      - Event Trace Sessions
      - Startup Event Traces
  - Reports
    - User Defined
      - New Data Collector Set
        - MBITT1\_1
    - System
      - Device Manager
- Storage
  - Disk Management
- Services and Applications

### Windows Trace Report

Computer: MBITT1  
Collected: 24 July 2017 09:28:31  
Duration: 7 Seconds

### Summary

Process		Disk	
<b>Total CPU%:</b>	15	<b>Top File by IO Rate:</b>	C:\PerfLogs\Admin\New Data Collector Set\MBITT1_20170724\Performance Counter.blg
<b>Top Process Group:</b>	audiodg.exe	<b>IO/sec:</b>	2
<b>Group CPU%:</b>	6	<b>Top Disk by IO Rate:</b>	0
<b>Total CPU%:</b>	1	<b>IO/sec:</b>	13
<b>Top Process Group:</b>			

### Application Counters

#### Processor

Top: 10 of 75

Performance Counter	Instance	Machine	Mean	Minimum	Maximum
% C1 Time	_Total	\\MBITT1	0.167	0	1.001
% C2 Time	_Total	\\MBITT1	83	63	88
% C3 Time	_Total	\\MBITT1	0	0	0
% DPC Time	_Total	\\MBITT1	0.056	0	0.39
% Idle Time	_Total	\\MBITT1	83	64	88
% Interrupt Time	_Total	\\MBITT1	0	0	0
% Privileged Time	_Total	\\MBITT1	4	1	14
% Processor Time	_Total	\\MBITT1	15	9	32
% User Time	_Total	\\MBITT1	10	8	19
C1 Transitions/sec	_Total	\\MBITT1	17	0	102

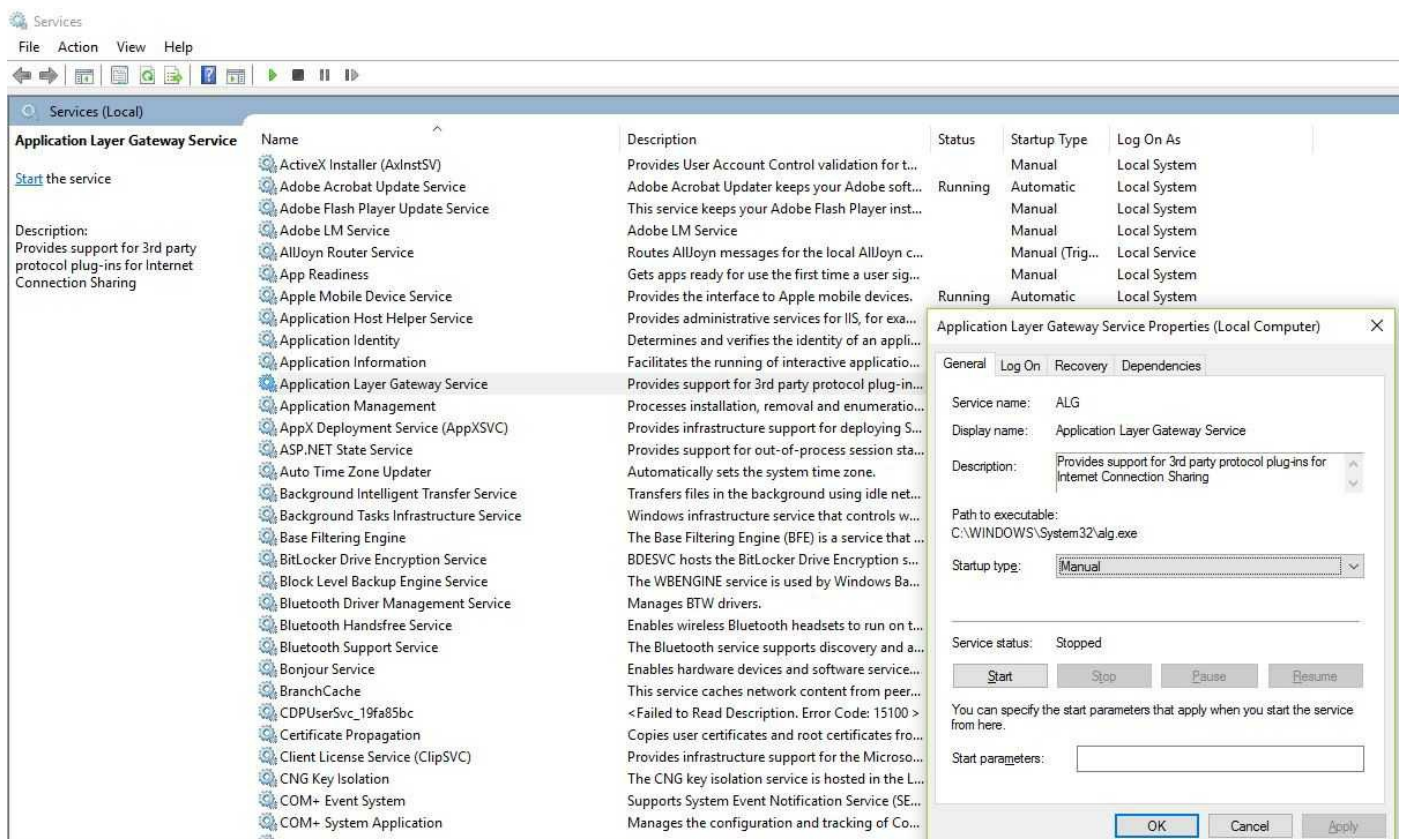
### CPU



# Services

The Services list is used to show all background services running on the system. From the service General tab you can stop, restart, and also set how a services will run. Services can be set to start manually, automatically (on startup), automatically with a delayed start (starts after login so as not to slow down the login process), or can also be disabled. The service needs an account to be assigned to it. This account defines who is running the service. This is not normally a user account, rather a system account. (Computers are very paranoid--it has its own account and has to give itself permission for a service to run!).

The Recovery tab is used to define what should happen if the service stops working. From here you can set if it will restart on the first attempt, run a program (for example, to alert the technician via email / SMS text) or restart the computer.







# System configuration

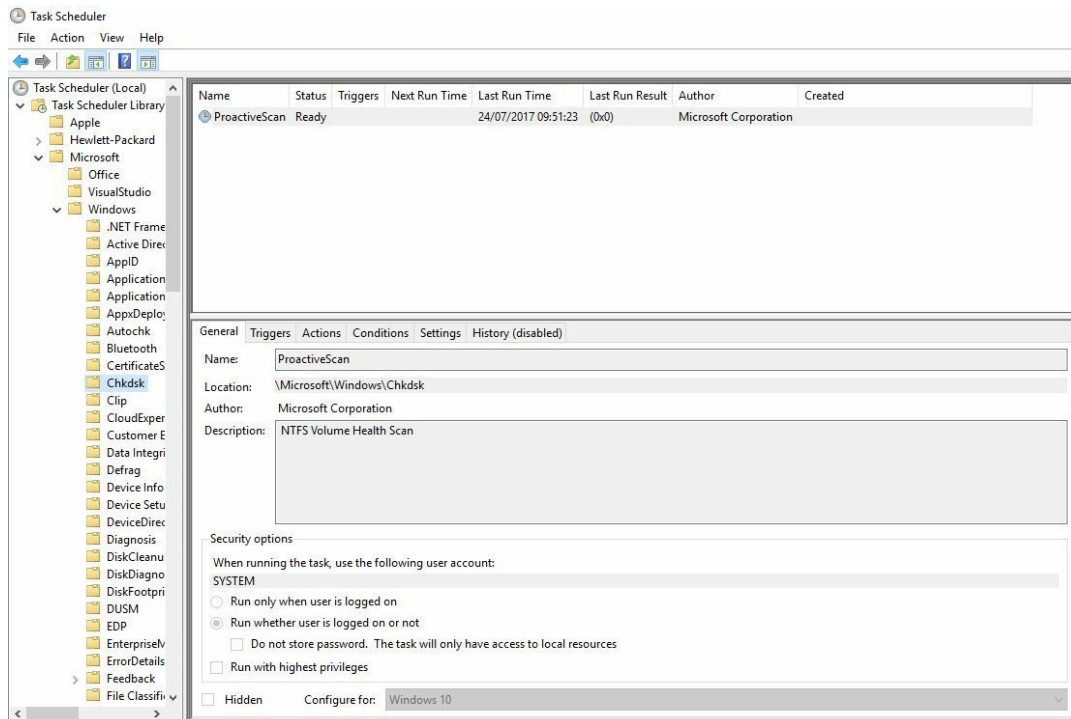
The System Configuration panel is designed to be a first stop for any technician to make key system changes. The filename to run this application is `MSCONFIG` and it is more commonly referred to as `MSCONFIG`. Please see the notes on `MSCONFIG` later in this chapter.





# Task scheduler

With Task Scheduler you can set a program or background service to start at a specific time and under a specific user / system account. You can set it to start daily or at specific times. This is extremely useful as with this you can set a backup, a defragmentation, or system cleanup to automatically run at a set time when users are not using the system (for example, at night, after normal work hours).

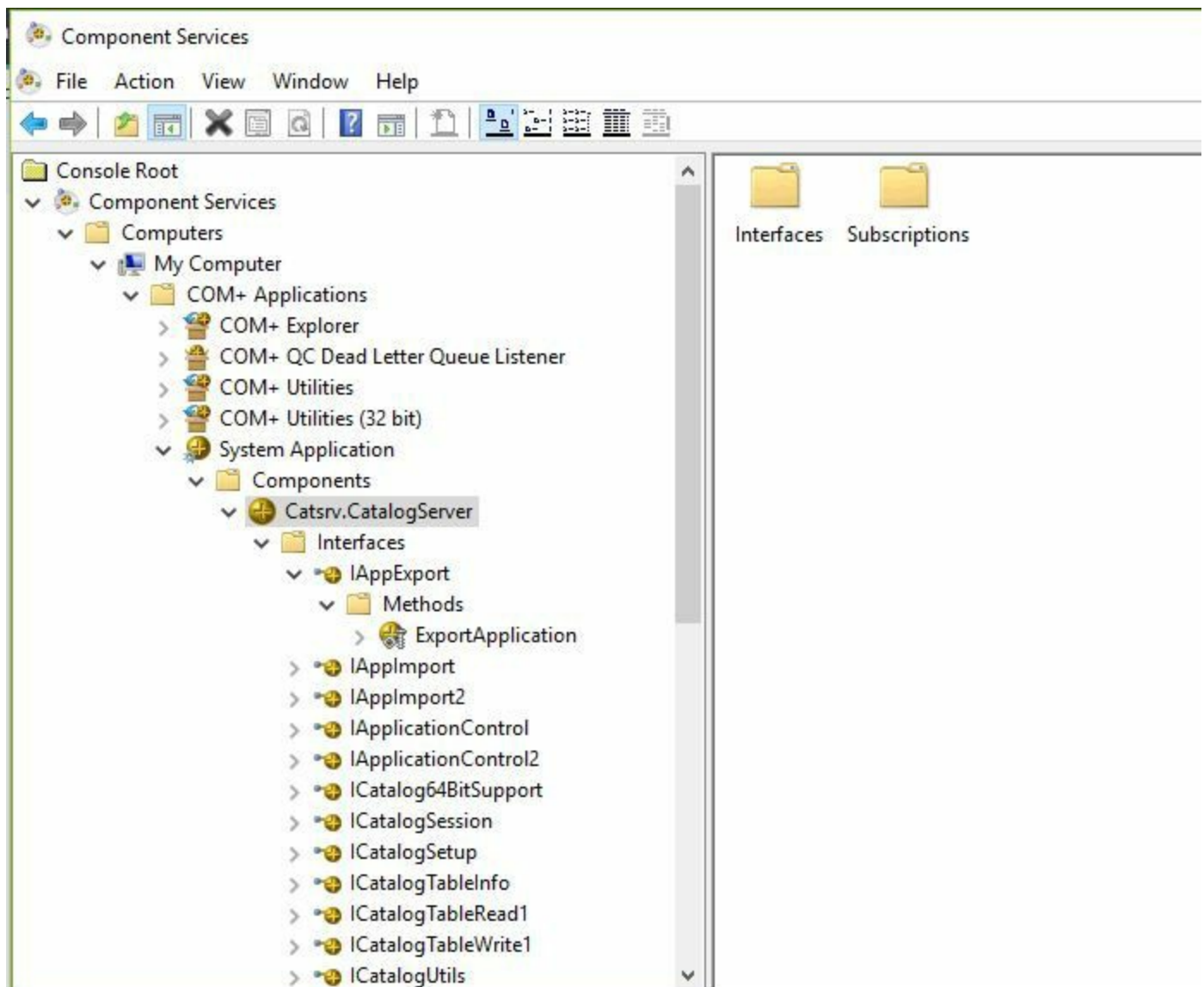




# Component services

The **Component Object Model (COM)** is a suite of low-level drivers and interfaces responsible for programs to be able to communicate with resources, or other parts of the system. The Component Services catalogue allows you to set the connections and startup context, also to alter the user / computer account used by a COM object.

It is highly advisable not to alter the COM settings. These are set during a software installation and rarely have to be changed.

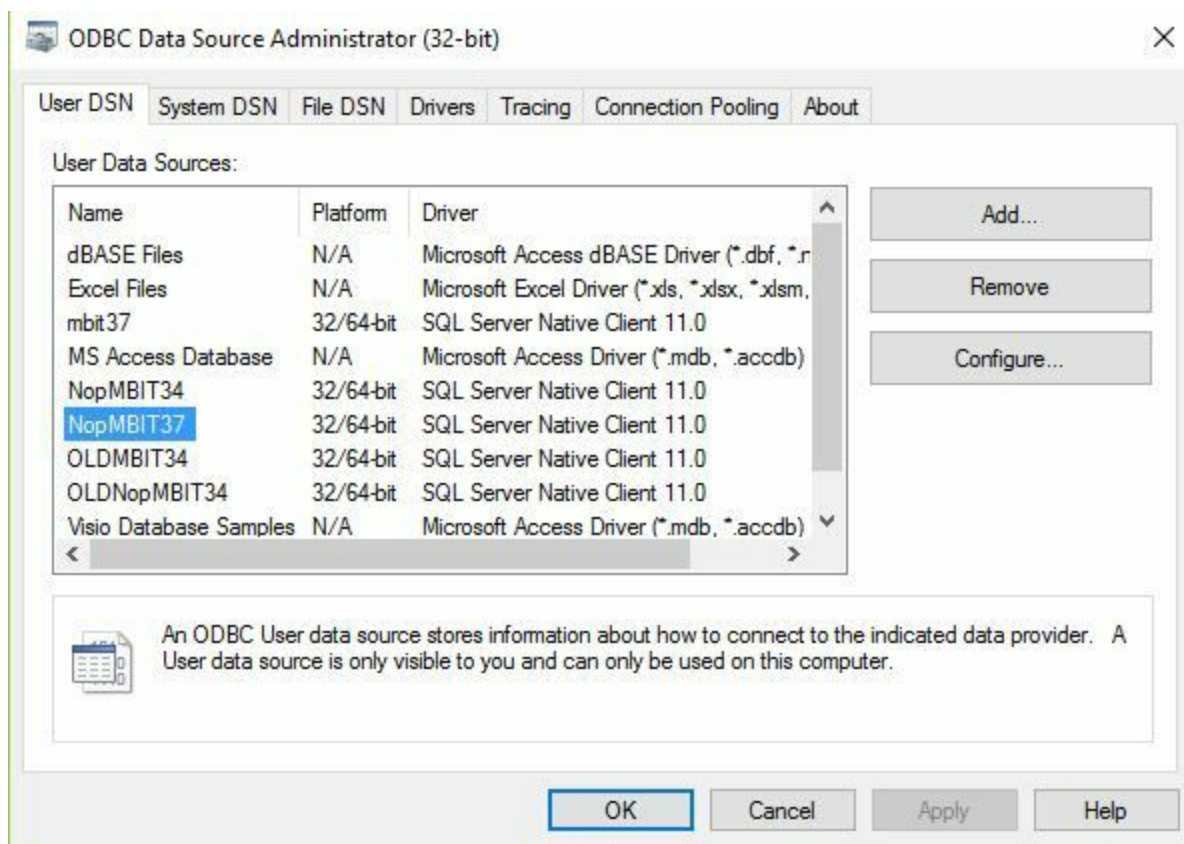




# Data sources

The ODBC Data Source administrator is a very old system designed to create low-level drivers used to connect to and interface with databases. These can be used to communicate with an SQL server database without the need of a SQL Server engine (for example, SQL Server Management Studio) present on the system. ODBC links allow you to also traverse the network and can be used to attach to network databases. However, there is an issue regarding security with ODBC and so ODBC has been superseded by using SQL connection strings (for example, ADO.NET) as the standard mechanism to connect to a database.

The ODBC pane comes as both 32-bit and 64-bit separately.

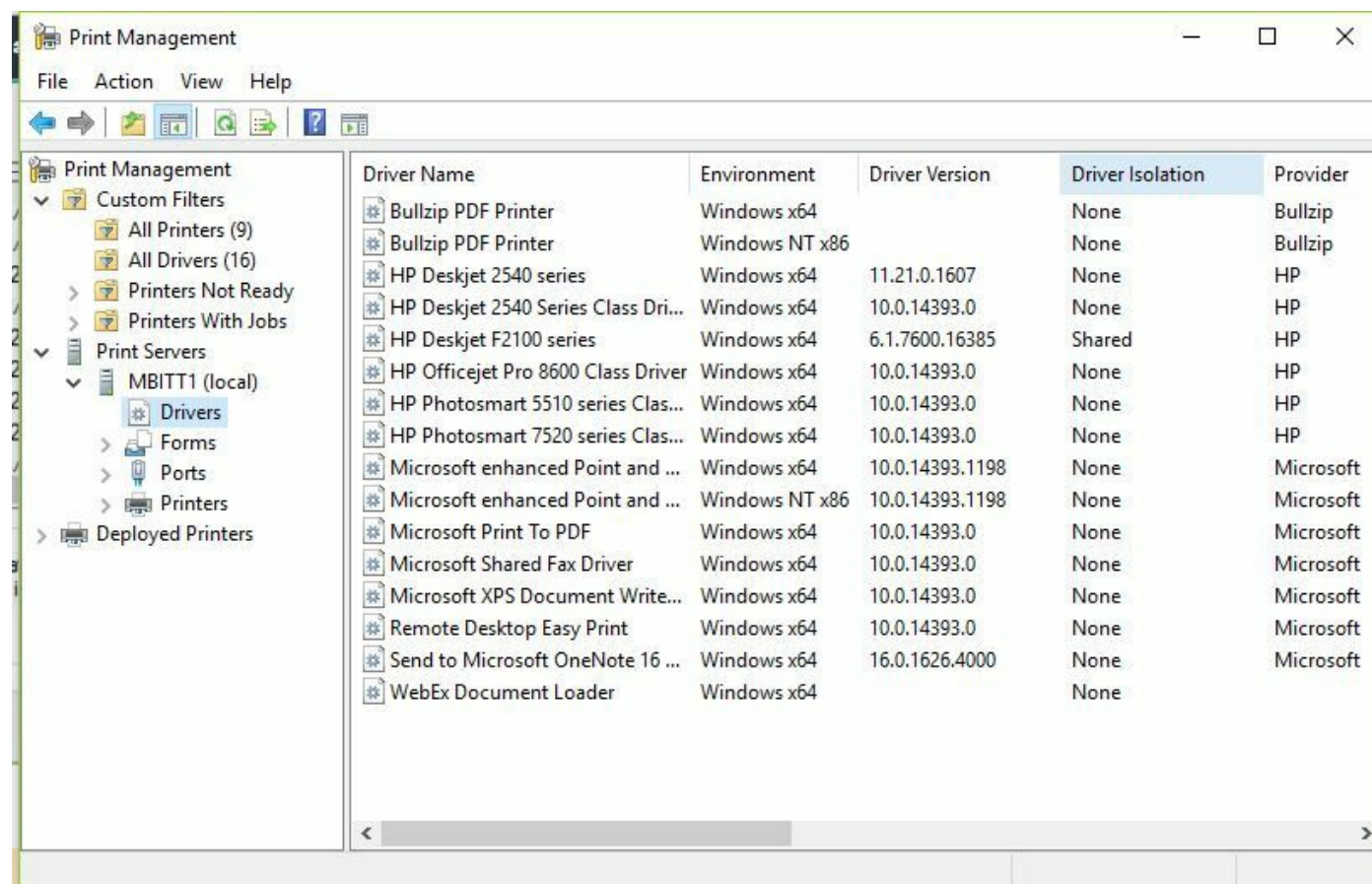






# Print management

The Print Management pane is a client-side version of the same tool found on Server 2012 when the Print Server role is installed. It lists all local printers, also drivers installed onto the machine (both 32 and 64-bit). This can be used as a central place to access print queues for printers that have stalled.





# Windows memory diagnostics

Slightly misleading by having the `Memtest` in the Admin Tools window--Windows Memory Diagnostics will perform a full scan of the RAM pages ensuring that each can be written to. However, as the OS is using a good portion of them you cannot perform a test whilst the OS is running. Triggering `Memtest` will cause the OS to restart into a low-level boot loader in which the memory test can safely run.

Memory testing tends to repeat until the end user cancels the test. If addresses cannot be written to or read the advice is simply to replace the affected RAM module. Quite often on new builds for performance reasons you need to check that the system remains stable after several hours of data transfers, so a Soak test is performed to check the hardware remains stable after (for example) 24 hours. I would advise against soak tests because the hardware has already been tested in the factory and you are simply wasting processing cycles and shortening the life of your hardware.



# Windows firewall

A Firewall is effectively a security screen. On the OSI model layer 4 (the Transport layer) we imagine that the TCP and UDP protocols both have a series of doorways, known as ports. These ports can be open inbound, outbound, or both. The port's status can be altered (or accessed) by a trigger such as if a particular program listed in a rule is running to open a specific port needed by that program.

There are two Firewall tools. Starting with the more basic Windows firewall, from here we can turn the firewall on or off and also set up the security for each profile separately. We have three profiles that can be used dependent on if the system is joined to a domain, acting either on a workgroup or as a standalone PC, finally it is connected to a public Wi-Fi access point (for example, in a coffee shop).

Typically the public profile is the most secure as you need to protect all resources from everyone else as they are untrusted. Domain uses different authentication mechanisms, but because they are used the Domain profile is the more relaxed security model.

With the basic firewall you can define which profile to use and also to allow an app through the firewall. Connection rules are made for you and that level of complexity is hidden from the user.









# Advanced security

A firewall on an Enterprise network is in fact quite an expensive piece of hardware that protects and screens all traffic entering or leaving the network. It can be found on the edge of the network and often is used to create an extra, semi-publicly accessible logical area of the network known as a **Demilitarized Zone (DMZ)**/Perimeter Network.

Software firewalls such as Windows Firewall/Firewall with Advanced Security work exactly the same way, but are used to protect the specific client PC. Each PC can have its own security settings that are different to the hardware Enterprise firewall box.

Advanced security allows me to create connection rules, both inbound and outbound for specific ports, setting a port as open / closed permanently or temporarily where the change is triggered by the starting or stopping of an application.

WFAS can also be used to create an encrypted connection tunnel protecting a resource and allowing encrypted traffic to the end device. These tunnels typically use L2TP to encrypt the tunnel (replacing the less secure PPTP) and also IPSEC to encrypt the packets sent through the tunnel. IPSEC can also be used to authenticate that the packets have come from the expected and reliable source. For this a certificate file has to be present at both ends of the tunnel.

Windows Firewall with Advanced Security									
File Action View Help									
Windows Firewall with Advanced Security									
Inbound Rules									
Name	Group	Profile	Enabled	Action	Override	Program	Local Address		
Altova License Metering Port (TCP)		All	Yes	Allow	No	Any	Any		
Altova License Metering Port (UDP)		All	Yes	Allow	No	Any	Any		
Apowersoft Screen Recorder Pro 2		All	Yes	Allow	No	C:\Progr...	Any		
Bonjour Service		Private	Yes	Allow	No	C:\Progr...	Any		
Bonjour Service		Private	Yes	Allow	No	C:\Progr...	Any		
Bonjour Service		Private	Yes	Allow	No	C:\Progr...	Any		
Bonjour Service		Private	Yes	Allow	No	C:\Progr...	Any		
Cain - Password Recovery Utility		Public	Yes	Block	No	C:\progr...	Any		
Cain - Password Recovery Utility		Public	Yes	Block	No	C:\progr...	Any		
Dropbox		All	Yes	Allow	No	C:\Progr...	Any		
Firefox (C:\Program Files (x86)\Mozilla Fir...		Private...	Yes	Allow	No	C:\Progr...	Any		
Firefox (C:\Program Files (x86)\Mozilla Fir...		Private...	Yes	Allow	No	C:\Progr...	Any		
HP Device Setup (HP Deskjet 2540 series)		All	Yes	Allow	No	C:\Progr...	Any		
HP Network Communicator COM (HP D...		All	Yes	Allow	No	C:\Progr...	Any		
imagej		Private...	Yes	Allow	No	C:\progr...	Any		
imagej		Private...	Yes	Allow	No	C:\progr...	Any		
iTunes		All	Yes	Allow	No	C:\Progr...	Any		
Microsoft Lync		Private...	Yes	Allow	No	C:\Progr...	Any		
Microsoft Lync		Private...	Yes	Allow	No	C:\Progr...	Any		
Microsoft Lync Ucmapi		Private...	Yes	Allow	No	C:\Progr...	Any		
Microsoft Lync Ucmapi		Private...	Yes	Allow	No	C:\Progr...	Any		
Microsoft Management Console		Private...	Yes	Allow	No	C:\windo...	Any		
Microsoft Management Console		Private...	Yes	Allow	No	C:\windo...	Any		
Microsoft Office Outlook		Private...	Yes	Allow	No	C:\Progr...	Any		
pluginhost.exe		Public	Yes	Allow	No	C:\users\...	Any		
pluginhost.exe		Public	Yes	Allow	No	C:\users\...	Any		
Sid Meier's Civilization V		All	Yes	Allow	No	I:\Games...	Any		
Sid Meier's Civilization V		All	Yes	Allow	No	I:\Games...	Any		
Skype		Private...	Yes	Allow	No	C:\progr...	Any		
Skype		Private...	Yes	Allow	No	C:\progr...	Any		
Steam		All	Yes	Allow	No	I:\Games...	Any		



# MSCONFIG

System Configuration is also known better by its filename--`MSCONFIG`.

The General tab is used to define how many of the startup drivers are used. If you have disabled some of the startup drivers then the setting will automatically be set to selective startup. The Boot tab shows the current Boot Configuration Database settings. From here you can see the number of OS systems on the boot list, define that the next time you boot the PC it will start in safe mode, switch off the Windows welcome graphic during booting (used to save a few seconds during the bootup process). The Services tab provides the list of loaded background services and their status. Startup used to (in Windows 7) show the list of programs which started up during login, however, this list has now been moved to Task Manager and replaced with a link to Task Manager. Finally, the Tools tab shows over 30 key tools from across the system and makes for a good menu to get to typical administrative tools you will need to use.



# Task Manager

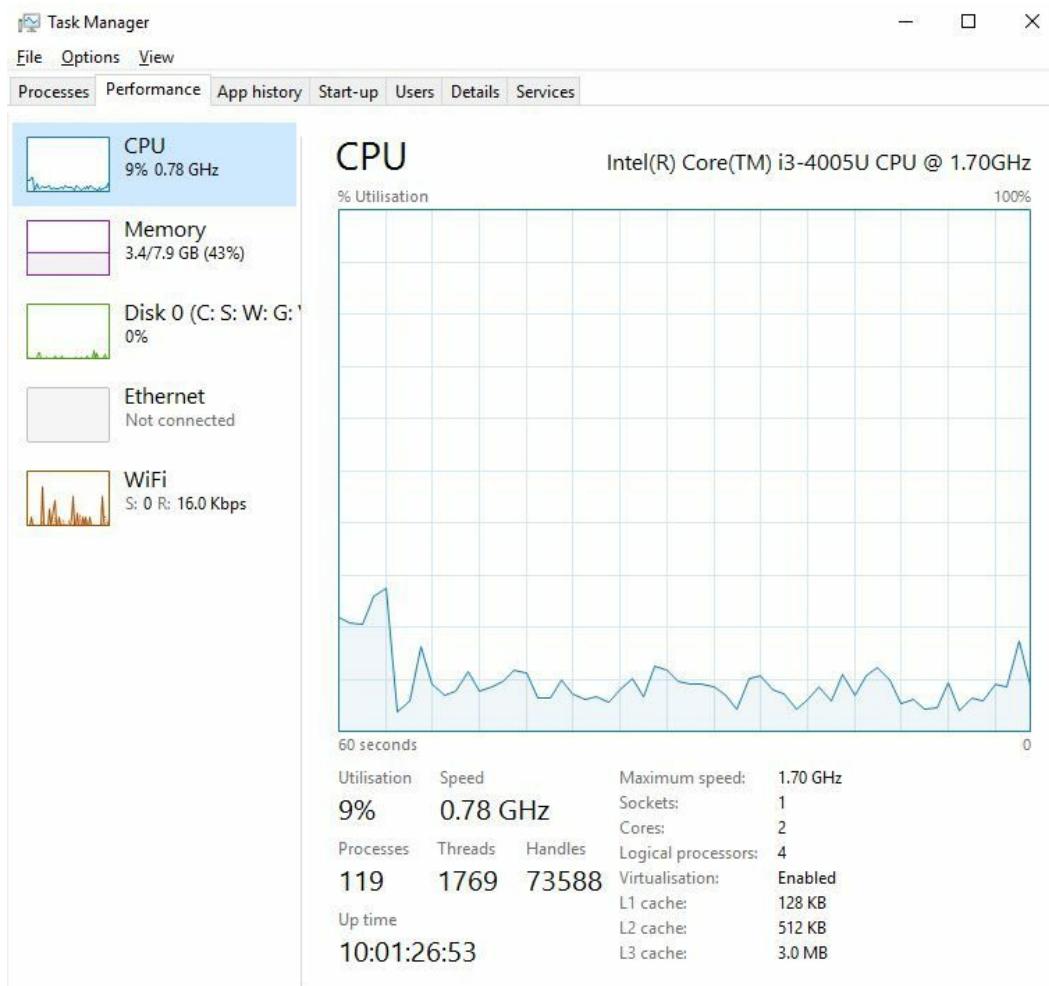
Task Manager provides a real-time account of how the system is performing and is your first tool to use to determine any problems with the system:

- Applications: The Applications tab is used to show running applications. On Windows 10 this now does not exist as a separate tab, but has been integrated into Processes.
- Processes: The Processes tab shows all running services and applications, how much processor time, memory, disk read/writes, and network throughput is dedicated to the application (as a percentage). These culminate as a total on the column heading. From this you can straight away determine if the PC is running hot and which component of the system is struggling. You can then determine which apps and services are causing a bottleneck and close them.

Name	26% CPU	43% Memory	1% Disk	0% Network
Apps (4)				
> Google Chrome	0.2%	55.4 MB	0.1 MB/s	0 Mbps
> Snipping Tool	0.1%	2.5 MB	0 MB/s	0 Mbps
> Task Manager	4.0%	18.0 MB	0 MB/s	0 Mbps
> Transport Empire (32 bit)	0%	232.8 MB	0 MB/s	0 Mbps
Background processes (71)				
> 64-bit Synaptics Pointing Enhance Service	0%	0.7 MB	0 MB/s	0 Mbps
> Adobe Acrobat Update Service (32 bit)	0%	0.4 MB	0 MB/s	0 Mbps
> Application Frame Host	0%	5.0 MB	0 MB/s	0 Mbps
> Bluetooth Radio Management Support	0%	0.5 MB	0 MB/s	0 Mbps
> Bonjour Service	0%	1.1 MB	0 MB/s	0 Mbps
> CCleaner	0%	4.7 MB	0 MB/s	0 Mbps
> COM Surrogate	0%	1.8 MB	0 MB/s	0 Mbps
> COM Surrogate	0%	3.3 MB	0 MB/s	0 Mbps
> Cortana	0%	85.9 MB	0 MB/s	0 Mbps
> Device Association Framework Provider Host	0%	7.2 MB	0 MB/s	0 Mbps
> Dropbox (32 bit)	0%	1.4 MB	0 MB/s	0 Mbps
> Dropbox (32 bit)	0%	1.2 MB	0 MB/s	0 Mbps
> Dropbox (32 bit)	0%	97.3 MB	0 MB/s	0 Mbps
> Dropbox Service	0%	1.5 MB	0 MB/s	0 Mbps

- Performance: The Performance pane provides a graphical overview of the four hardware elements, also with a sub-pane reporting on (for example, for the CPU

section:) Utilization, Uptime, Speed, Sockets, Cores, caching, if virtualization has been enabled in the BIOS as well as an exploded graphical chart covering CPU usage (as a percentage) over time.



- **App history:** This is a new table available in Windows 10 that shows how long a store app has been used for and also how much data has been transferred over a metered connection. This is useful for laptop users who access mobile data through their phone when working away from the office, to determine which apps are downloading background data without your knowledge.
- **Start-up:** The Start-up tab shows all applications that have at some point been set to start up during login. Here you can enable/disable apps for the current session running.
- **Users:** This pane breaks down the running apps and services listing which user account has called them to be executed. The apps / processes run against the user profile, so if you have multiple users signed in on the PC you can see which user is using more resources on the system.
- **Networking:** The Networking tab shows a graphical display of network usage.

However, this no longer exists in Windows 10 as it has been integrated into the Performance tab.

- Details: Similar to the Processes tab, but the Details tab also provides the Processor ID for the running app. Where an application is in fact subdivided into a group of apps each will have their own memory space and PIDs.
- Services: The Services tab shows the existing service profile and allows you to start or stop services; however, this is only for the existing session. You are still advised to use the main `Services.msc` and not the `Task Manager - Services` tab.





# Disk management

Disk Management is a powerful tool allowing you to mount new hard disks, initialize them, set partitions, format these partitions, shrink or expand partitions, extend the capabilities of the disk to create more complex volumes such as spanned partitions, or a RAID array.

All of these actions can also be achieved through the Command-Line tool: `DISKPART` which can also be used to set active partitions, hide partitions, and other low-level disk maintenance.

The disk is displayed as a bar chart listing the partitions, their types, and sizes.



# Drive status

A drive can either be:

- **Online:** The disk is working and accessible. In the Storage Spaces context this is referred to also as healthy.
- **Not Initialized:** The disk is ready to be used by the OS, but currently the disk is not registered with the OS, meaning that Windows does not have permissions to manage the disk. Initializing registers the disk's ID in the registry allowing Windows permission to access the disk. Windows ID data is also written to the front of the disk. A basic disk always starts off as not initialized. CD/DVD ROM drives are Online by default.
- **Foreign:** When Windows allows a disk to be accessible the Windows ID data is written onto the disk. If the disk is transferred to another PC, on the new PC Windows will notice the ID stamp from the earlier OS and recognize that the disk is Foreign. As an administrator you can then initialize the disk replacing the ID stamp with the new OS, allowing the OS to control the disk.



# Mounting

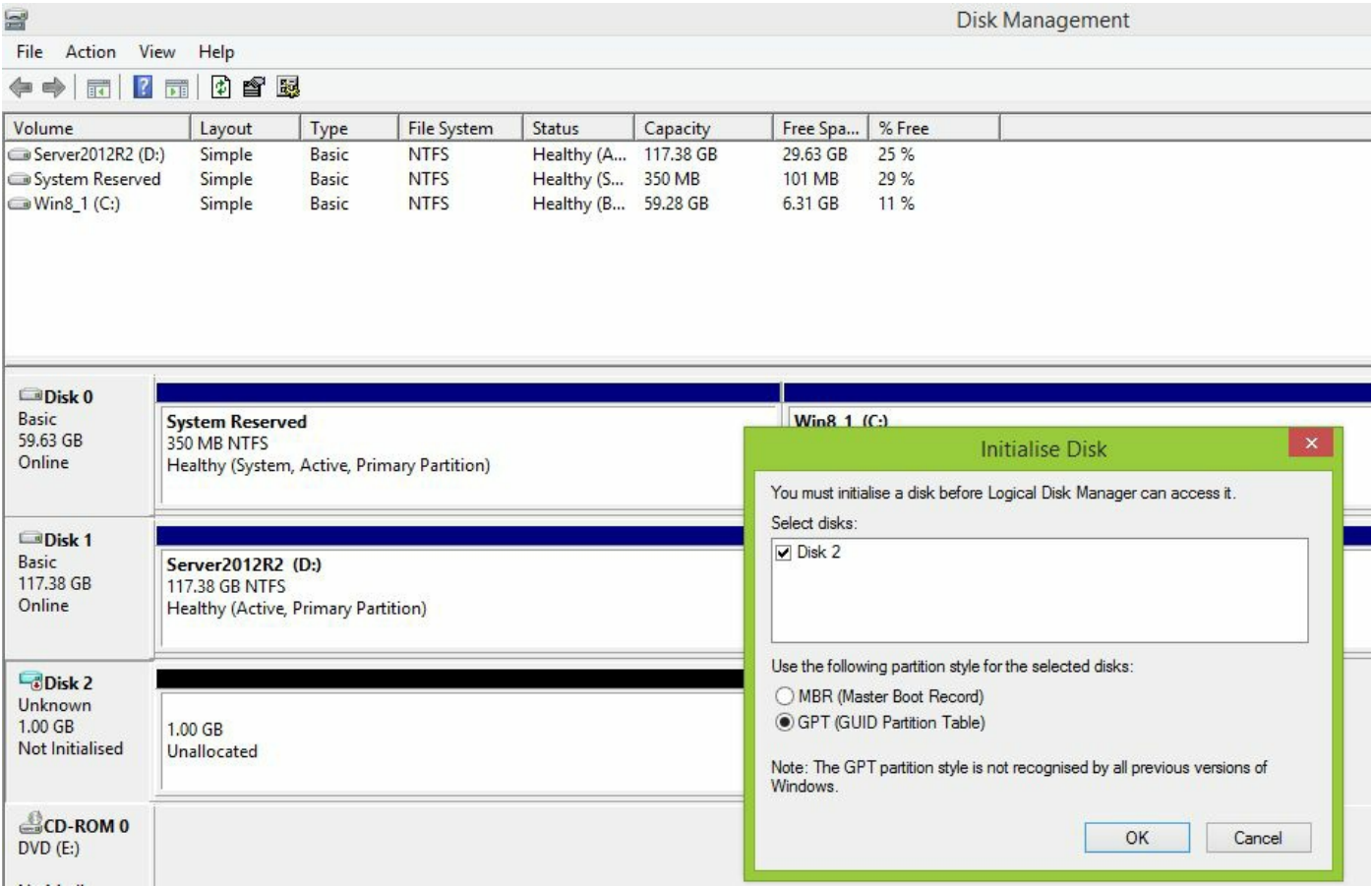
Mounting is a process of connecting a volume or mount point to a new partition to use as part of that volume. Typically we mount by ensuring that the partition is formatted, viewable (not hidden) and has a drive letter. If we are extending space for an existing partition by adding space as a new folder we create a new folder on the old volume and then attach the new partition as extra space for the new folder to use. This is commonly used when you have an existing, almost full volume and want to store a large amount of files such as a music library typically to be stored on another physical disk. The enduser will see the folder, but no discernible change yet that folder will be able to store a large amount of data.

External devices such as external storage, USB pen drives, or CD-ROMs have to be mounted before use. This is an automatic process with Windows, but it has to be unmounted manually before they are disconnected to avoid loss of data.



# Initializing

The process of allowing Windows to control a disk otherwise marked as Not Initialised or Offline is to initialize the disk. This gives Windows permission to control the disk.







# Extending partitions

In Disk Management the right-hand partition market can be extended further into unused space to the right of the block. With NTFS and Dynamic Disks using the GPT you can also extend into non contiguous space (for example, Volume C, Volume F).

You cannot, however, extend into unused space to the left of the block and would need to move the block that needs to be done using third-party software such as Disk Commander. This is very dangerous and not recommended. The alternative would be to:

1. Move the block to the right of the disk into unused space.
2. Make a new volume in the now free space and `ROBOCOPY` the files over from the old volume into the new one.
3. Delete the old volume.
4. Change the drive letter back to the old letter used.



# Splitting partitions

Splitting a partition means to divide an existing partition into two and a new volume letter assigned to the second partition. This is not possible in Disk Management using the existing tools, rather the alternative would be to shrink the existing partition back to the size you want the resulting volume to be, and then create a new partition for the next volume in the now unused space gap. You will of course need to move any files out of the way that otherwise may stop the shrinking taking place.



# Shrink partitions

Shrinking a partition is quite straightforward. Simply select the partition to shrink and in the wizard state by how much you wish to shrink it. The partition is resized by moving the right partition handle to the left.



# Assigning/changing drive letters

Simply right-click on the volume and select Change drive letter and paths to alter the volume letter.





# Adding drives

Drives are not added through Disk Management. Once a drive has been added to the system it will appear as a new drive in Device Manager and as an unmounted drive in Disk Management. You need to initialize the disk first and specify if we are going to use MBR or GPT as the partitioning table after which point partitions can be created, formatted, and labeled.

Virtual Hard Disks can also be added as though they were physical drives through the Add menu. Through here you can also create new VHD rather than using the Hyper-V Manager to create one.



# Adding arrays

You will need several unformatted, unpartitioned, initialized disks to create an array. These disks will need to be set as dynamic disks to support advanced arrays such as RAID. The array is created by right-clicking in the unused space within the first disk in the array. From here you can specify which disks to use and the type of array you can create:

Volume choices are:

- **New Simple Volume:** A volume existing on one disk only.
- **New Striped Volume:** A RAID 0 software equivalent. Data is saved to both disks in the array at the same time increasing performance. Both disks need to be present for the volume to be accessible.
- **New Spanned Volume:** A volume starting on one disk, but additional volume data is saved to the second allocated disk.
- **New Mirrored Volume:** A RAID 1 software equivalent. The same data is saved to both disks in the array at the same time. There is no performance benefit, but you get fault tolerance should one disk fail as the volume will still be readable.
- **New RAID5 Volume:** A RAID 5 software equivalent. Data is saved to both disks in the array at the same time increasing performance and a third parity bit (Checksum) is saved to the third disk. The roles cycle around and the parity bit is saved to a different location each time. Two of three disks need to be present for the volume to be accessible meaning that you can recover from one single disk failure. The volume will need to be regenerated as the OS works out the data missing from the damaged disk. This is done by removing the damaged disk and replacing it with a new one, but the gaps in the volume need to be calculated. As you cannot reverse engineer from the checksum it takes a lot of calculation to determine the missing pieces and regenerate the volume which can take several hours.



# Storage spaces

Now part of Server 2012 and also available in Windows 10 the Storage spaces feature is an adaptation of the RAID principle. Here we separate out the physical disks and the logical volume we are going to create in the system. Furthermore, I can now create a volume much larger than I actually have as the physical limitation based on the size of the disks in the array is no longer a prerequisite for making a volume. As the volume expands and fills the disk other disks are added to the Storage Pool until the pool is full at which time the system will prompt you to add more disks.

A number of new concepts are in place with Storage Spaces:

- This is designed to support SAN rack-mounted hard drive caddies where there are a series of hot-swappable, powered and ready hard disks waiting to be used. They are added to a basic Storage Pool called the Primordial and we take disks either automatically or manually from the pool to add to a new Storage Pool group. From this a Virtual Disk (a logical disk representing all of the physical disks in the storage pool and viewable to the OS) is used - the OS only sees one disk. From this we can create a volume linking to the virtual disk.
- RAID is possible as a Two-way Mirror where three disks are used (the original, one mirror to the left, one mirror to the right). These can support one disk failure and the mirror will also still work. A three-way Mirror commonly uses five disks - it can support two disk failures and have the mirror still running, but also uses a spare.
- If the storage space volume is thin-provisioned, data is added to the volume as and when needed. With Fixed-Provisioned the actual volume size's worth of space is needed from the outset. This is often used in situations such as SQL, IBM, or Oracle databases where the area is designated to the Database engine to save its data into the volume, not Windows.



# Other tools

In the 901 course we covered the concept of moving user data from one PC to another. If you are planning to replace the existing hardware you will need to take a copy of the current user states and load these onto the new PC. Windows Easy Transfer is a tool built into the installation DVD that can be run on the older system (for example, Vista). It replaces XP's File and Transfer Wizard by copying the state and contents of one user account onto an archive file. This file can then be loaded onto the new PC where the user account will be imported.

To decide if the existing hardware will support an upgrade it is advisable to download and run the Windows Upgrade Advisor located here (<https://www.microsoft.com/en-gb/download/details.aspx?id=20>). Things are less straightforward with 8.1 or 10 though as later advisors are integrated into Windows updates. Its job is to produce a report detailing if your existing system will support an upgrade, or if components need to be refreshed.

If you want to copy several user accounts this can be done as a batch process. The USMT exists as part of the Microsoft Deployment Toolkit and is also available separately here (<https://www.microsoft.com/en-gb/download/details.aspx?id=10837>). This consists of two commands - `SCANSTATE` is a command-line tool run on the old (reference) PC and creates an encrypted archive file. A typical `SCANSTATE` command would be:

```
| scanstate.exe c:\backup /o /all /c /auto /l:"c:\scanstate.txt" /localonly
```

`LOADSTATE` is its equivalent run on the new PC (the target PC). The archive file must exist in a folder on the local PC:

```
| Loadstate.exe /i:"C:\backup" /hardlink /nocompress
```

As these are to create local accounts I often also use the switches `/lac` (local account create) and `/lae` (local account enable) as local accounts are created, but deliberately disabled until they are needed.





# System utilities

In this section, we are going to cover some of the other GUI and CLI tools that are very important and in fact integral to the system, but do not fall into a specific category. Some of these are referred to as under the bonnet given that they should be kept away from the end user who if they knew existed may damage their OS.



# REGEDIT

The Registry Editor is a database of all of the configurations set for every aspect of the OS. The configurations are split into various folders known as hives. These hives contain the different configuration areas:

- **HKEY\_CLASSES\_ROOT**: This is a list of file extensions and tells the OS which application to use to open this kind of file
- **HKEY\_CURRENT\_USER**: These are the configuration settings for the user currently logged on.
- **HKEY\_LOCAL\_MACHINE**: This is the full list of computer configuration settings that may be used on the current PC.
- **HKEY\_USERS**: These are the configuration settings for every user account set up on this PC.
- **HKEY\_CURRENT\_CONFIG**: These are the configuration settings for the existing computer account.

When a user logs in the current user and current configuration settings are loaded with the settings from the Local Machine and Users areas for the user who has signed in.

A useful feature built into the F8 advanced boot menu is the Last Known Good option. Have you ever made a change to your machine, restarted the PC, and then regretted making the change, and because of the settings change cannot revert back? As long as you realize your mistake before you log in, then the Last Known Good option does not replace the Current User settings with the user settings stored in the Users hive, rather continues to use the Current User settings for your new login. In this way you log in to an account at a point in time before the configuration settings were saved. Logging out will save the user profile back to the Users hive and effectively undo the erroneous change that you made to the system.

It is appallingly dangerous to edit the Registry directly. Most of the configuration settings and DWORD values have been set by the system and a number of these modular subfolders comprise the OS as a whole. One slight change that is not recognized can lead to system instability.

# Registry Editor

File Edit View Favorites Help

Computer	Name	Type	Data
<ul style="list-style-type: none"> <li>HKEY_CLASSES_ROOT</li> <li>HKEY_CURRENT_USER                             <ul style="list-style-type: none"> <li>AppEvents</li> <li>AppXBackupContentType</li> <li>Console</li> <li>Control Panel</li> <li>Environment</li> <li>EUDC</li> <li>Keyboard Layout</li> <li>Network</li> <li>Printers</li> <li>SOFTWARE</li> <li>System</li> <li>Volatile Environment</li> <li>WXP</li> </ul> </li> <li>HKEY_LOCAL_MACHINE                             <ul style="list-style-type: none"> <li>BCD00000000</li> <li>HARDWARE</li> <li>SAM</li> <li>SECURITY</li> <li>SOFTWARE</li> <li>SYSTEM                                     <ul style="list-style-type: none"> <li>WindowsAppLockerCache</li> </ul> </li> </ul> </li> <li>HKEY_USERS</li> <li>HKEY_CURRENT_CONFIG                             <ul style="list-style-type: none"> <li>Software</li> <li>System</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>(Default)</li> <li>DNX_HOME</li> </ul>	<ul style="list-style-type: none"> <li>REG_SZ</li> <li>REG_SZ</li> </ul>	<ul style="list-style-type: none"> <li>(value not set)</li> <li>%USERPROFILE%\dnx</li> </ul>
	PATH	REG_EXPAND_SZ	C:\Users\Matthew\dnx\runtimes\dnx-clr-win-x86...
	Pythonpath	REG_SZ	C:\Python27\;C:\Python27\Scripts;
	TEMP	REG_EXPAND_SZ	%USERPROFILE%\AppData\Local\Temp
	TMP	REG_EXPAND_SZ	%USERPROFILE%\AppData\Local\Temp



# COMMAND

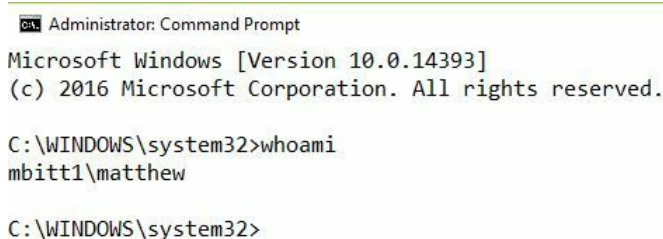
Also known as and called by CMD, the Command Console is a DOS command window allowing you to make system changes using the CLI. Typically opening this opens a restricted version - any changes to the OS that will require system approval require elevated privileges. To do this right, click on the CMD icon and select Run as Administrator.

The Command window accepts DOS and UNIX commands that are still resident on Windows systems (such as the `NET` and `NETSH` commands).

PowerShell can also be loaded by typing `PowerShell` into the command window. Through here a PowerShell session will start and we will be able to use PowerShell commands instead of DOS ones. To exit to the DOS CLI, type `Exit`.

On Servers, CMD is deprecated and PowerShell has replaced it. PowerShell can also run most DOS commands, but does so using a PowerShell alias so the results and output may look a little different to what you are used to.

A CMD prompt can also be triggered from the jump list, right-clicking the Windows Start button.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>whoami
mbitt1\matthew

C:\WINDOWS\system32>
```





# SERVICES.MSC

The Services console lists all background services and their status. We have looked at this earlier - it can be accessed from the `Run` command using the preceding Microsoft Console file. This is the preferred method to view and edit the services list as it affects all logged on users, whereas Task Manager's services page is contextual.

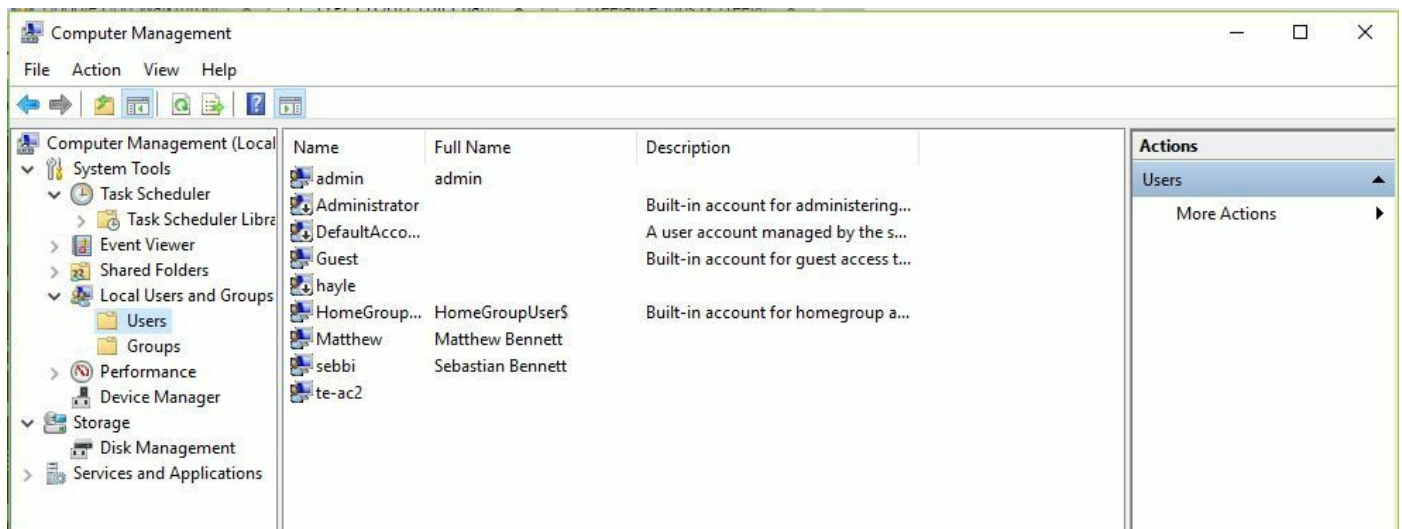


# MMC

This is one of the most important commands you as a technician need to know, when working with Microsoft systems. The MMC is a GUI window allowing you to access several hundred different GUI tools. An example of some of these tools is actually the Computer Management window that has some of the key tools used by technicians to perform routine configuration tasks.

One advantage of the MMC is that once you have added the snap-ins you need, you can save the MMC as a tiny file that can then be opened on other PCs. I tend to travel with a USB pen drive on which I have a pre-configured MMC with all of the snap-ins I need to use.

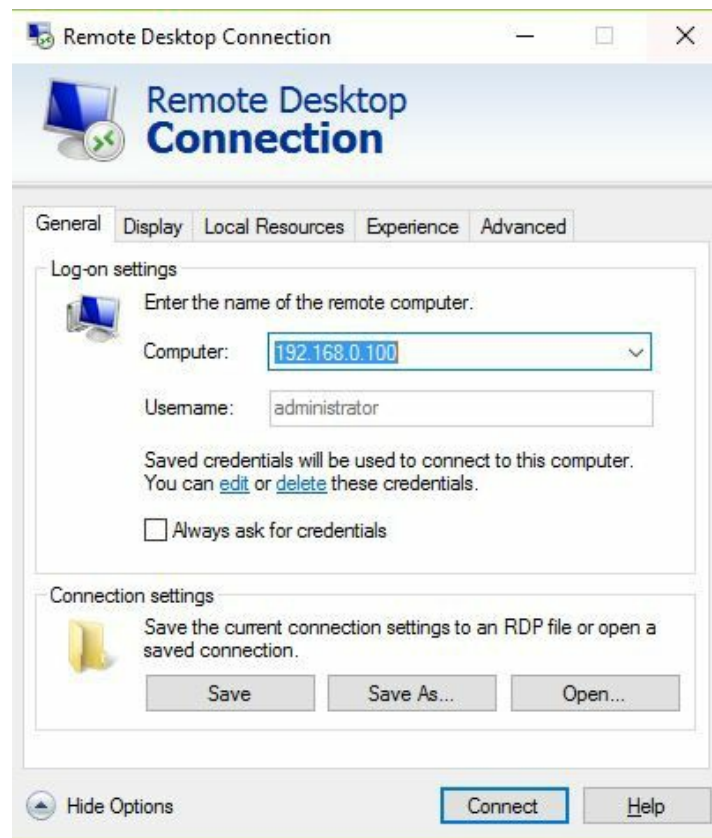
Another advantage of the MMC window is that when you select a snap-in you get the choice to receive data about the local computer, or can obtain data from another computer on the network. For this you will need Remote Management to be enabled on the remote computer, but it saves having to physically walk to and work on the remote PC.





# MSTSC

Microsoft Terminal Services Console (to give it its proper title) is better known by Remote Desktop Connection. With this you can obtain a window allowing you to connect to another PC on the network. Remote Desktop can stream the audio from the remote PC and you can also share your local devices such as connected external drives, floppy disk drive, or local printer with the remote PC. You can set the session video resolution and even create an RDP file containing your username so that if you need to access the remote PC again you simply click on the RDP file on your desktop.



The certification exam will ask you about some of the additional tabs within the Remote Desktop Connection, especially on how to connect local hardware to the remote PC and how to change the user experience to simulate a slow link. Practice with these to discover how they work for yourself by remoting to another PC on your home network.



# NOTEPAD

Whilst there are third-party equivalents such as the immortal Notepad++ used by a wide variety of developers, Notepad is itself a basic text editor allowing you to create a text file and add basic formatting.

I tend to place text I have copied from an app or website into Notepad first, and then re-copy it to then add it to the destination app. By doing so Notepad will strip out any formatting that you don't want in your destination app.

Notepad is limited by the size of the file you can open to only a few KB. For larger documents consider WordPad (the built-in Rich Text editor).

Notepad is also useful when viewing information sent unencrypted across the network, or to see a file intended for other formats such as a DOCX file for Word as here you will be able to extract content when you do not have access to the application the file was intended for.





# EXPLORER

Known as File Explorer and formerly Windows Explorer, this is a hierarchical tree of your volumes and their respective files and folders. All basic file manipulation DOS actions can also be done here and in fact Explorer is the preferred tool for most IT technicians for CRUD operations (Create, Read, Update, Delete).

The exam assumes that you already know how to manipulate files using Explorer, also that you know to snap two explorer panes and can drag and drop with the mouse to copy or to paste a file or multiple objects from one location to another. The exam will instead consider two areas:

- **Encrypt or Compress:** Blue files are compressed, green are encrypted. With Windows 10 we do not use the colors, rather a tiny icon in the top right of the file icon. A blue double-arrow indicates compressed and a gold padlock indicates that the file is encrypted. A file can be one or the other, but not both. No additional icon (in Windows 10) or black text (in earlier systems) indicates that the file has no additional properties.
- **Move or Copy:** There are different behaviors depending on where you are sending the file to. On NTFS volumes the file's security permissions are changed depending on if you move or copy the file.

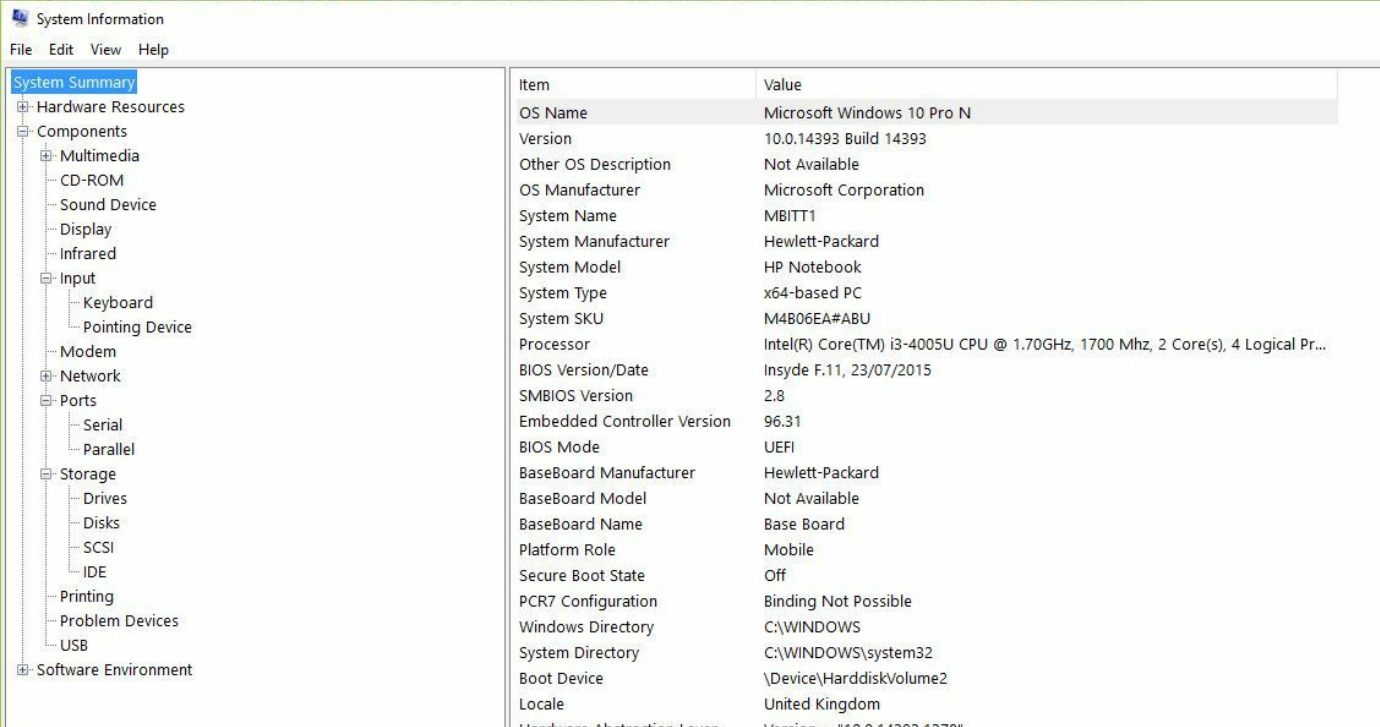
When you copy a file or folder within an NTFS partition, the file or folder inherits the compression state of the target folder. For example, if you copy a compressed file or folder to an uncompressed folder, the file or folder is uncompressed automatically. When you move a file or folder within an NTFS partition, the file or folder retains its original compression state. For example, if you move a compressed file or folder to an uncompressed folder, the file remains compressed. When you move a file or folder between NTFS partitions, the file or folder inherits the target folder's compression state. Because Windows 10 treats a move between partitions as a copy followed by a delete operation, the files inherit the target folder's compression state. When you copy a file to a folder that already contains a file of the same name, the copied file takes on the compression attribute of the target file, regardless of the compression state of the folder. Compressed files that you copy to a FAT partition are uncompressed because FAT volumes do not support compression. However, when you copy or move files from a FAT partition to an NTFS partition, they inherit the compression attribute of the folder into which you copy them. Microsoft Official Course 20697-1C Implementing and Managing Windows 10 Student Guide.





# MSINFO32

System Information is a detailed report listing all hardware and software components plus all configuration settings for the existing PC. From here you can determine the architecture plus the make and model of hardware components where they are known by the system, where generic drivers have not been installed. Third-party equivalents would be Everest or SiSandra.

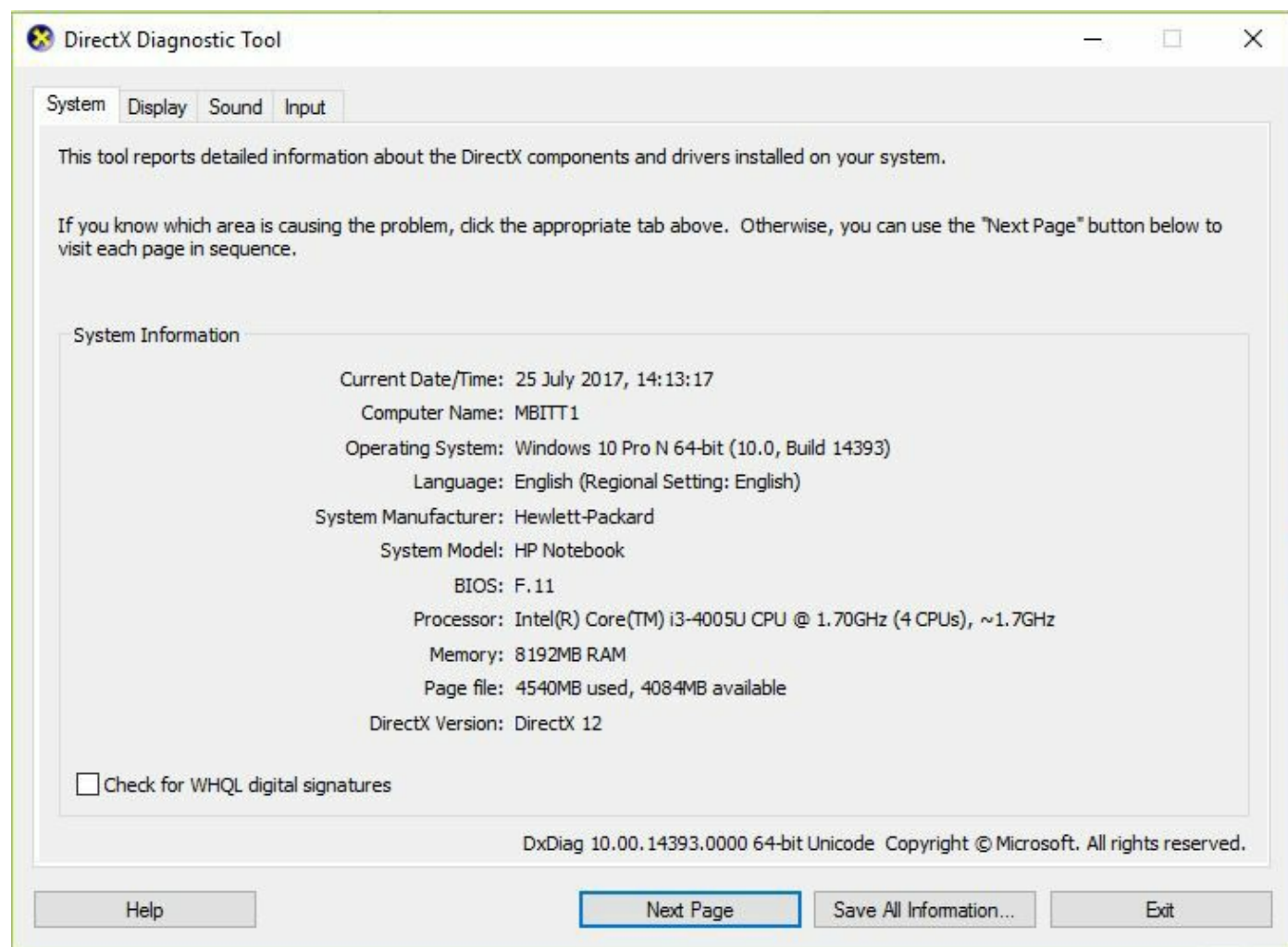


Item	Value
OS Name	Microsoft Windows 10 Pro N
Version	10.0.14393 Build 14393
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	MBITT1
System Manufacturer	Hewlett-Packard
System Model	HP Notebook
System Type	x64-based PC
System SKU	M4B06EA#ABU
Processor	Intel(R) Core(TM) i3-4005U CPU @ 1.70GHz, 1700 Mhz, 2 Core(s), 4 Logical Pr...
BIOS Version/Date	Insyde F.11, 23/07/2015
SMBIOS Version	2.8
Embedded Controller Version	96.31
BIOS Mode	UEFI
BaseBoard Manufacturer	Hewlett-Packard
BaseBoard Model	Not Available
BaseBoard Name	Base Board
Platform Role	Mobile
Secure Boot State	Off
PCR7 Configuration	Binding Not Possible
Windows Directory	C:\WINDOWS
System Directory	C:\WINDOWS\system32
Boot Device	\Device\HarddiskVolume2
Locale	United Kingdom
Hardware Abstraction Layer	Version - "10.0.14393.1378"



# DXDIAG

The graphics card supports the DirectX code framework that is used to render advanced graphics by the system. Most modern apps and also games require either the open standard (OpenGL) or Microsoft's own DirectX architecture to be present to be able to manipulate and draw graphics. DirectX is a family of software products: Direct3D, DirectDraw, graphics acceleration features but also MIDI and input devices such as joysticks can use the DirectX suite.



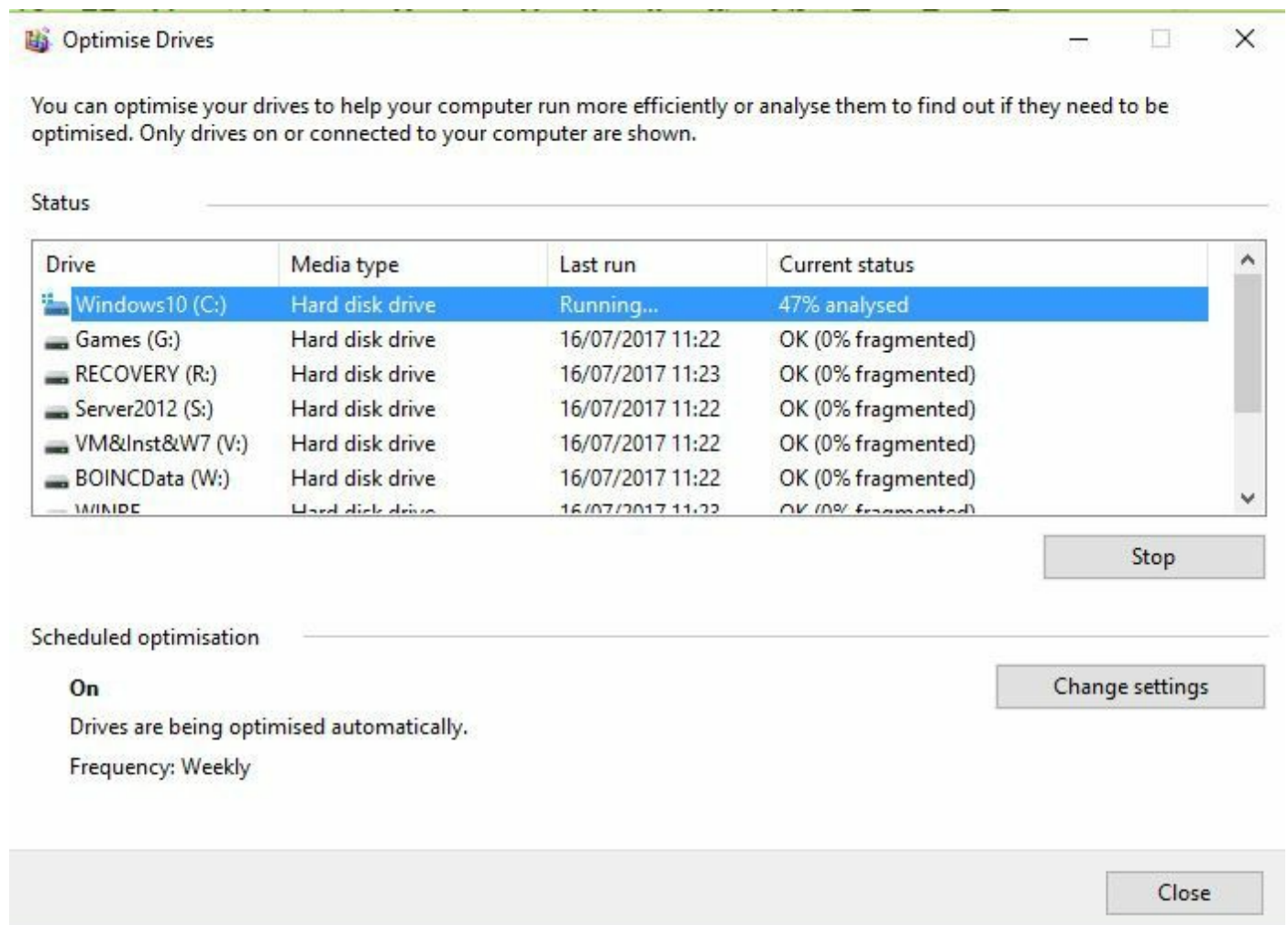


# DEFRAG

Over time the system will split files across blocks where there is space on the hard disk, but although it tries to keep the data in adjacent blocks, it cannot always manage to do so and this leads to fragmentation. The file has to be re-pieced back together in memory before it can be used, so accessing the blocks and retrieving the file slows down the more fragmented the disk becomes. Defrag is a built-in tool to remedy this by retrieving the file and re-saving it into contiguous space on the hard disk, improving disk-read performance.

There are third-party tools that also provide a graphic drive map, but Defrag is equally as good.

From Windows 8 onwards the system will perform automatic weekly scans of your drive. On earlier versions this had to be configured as a scheduled task, or run manually.



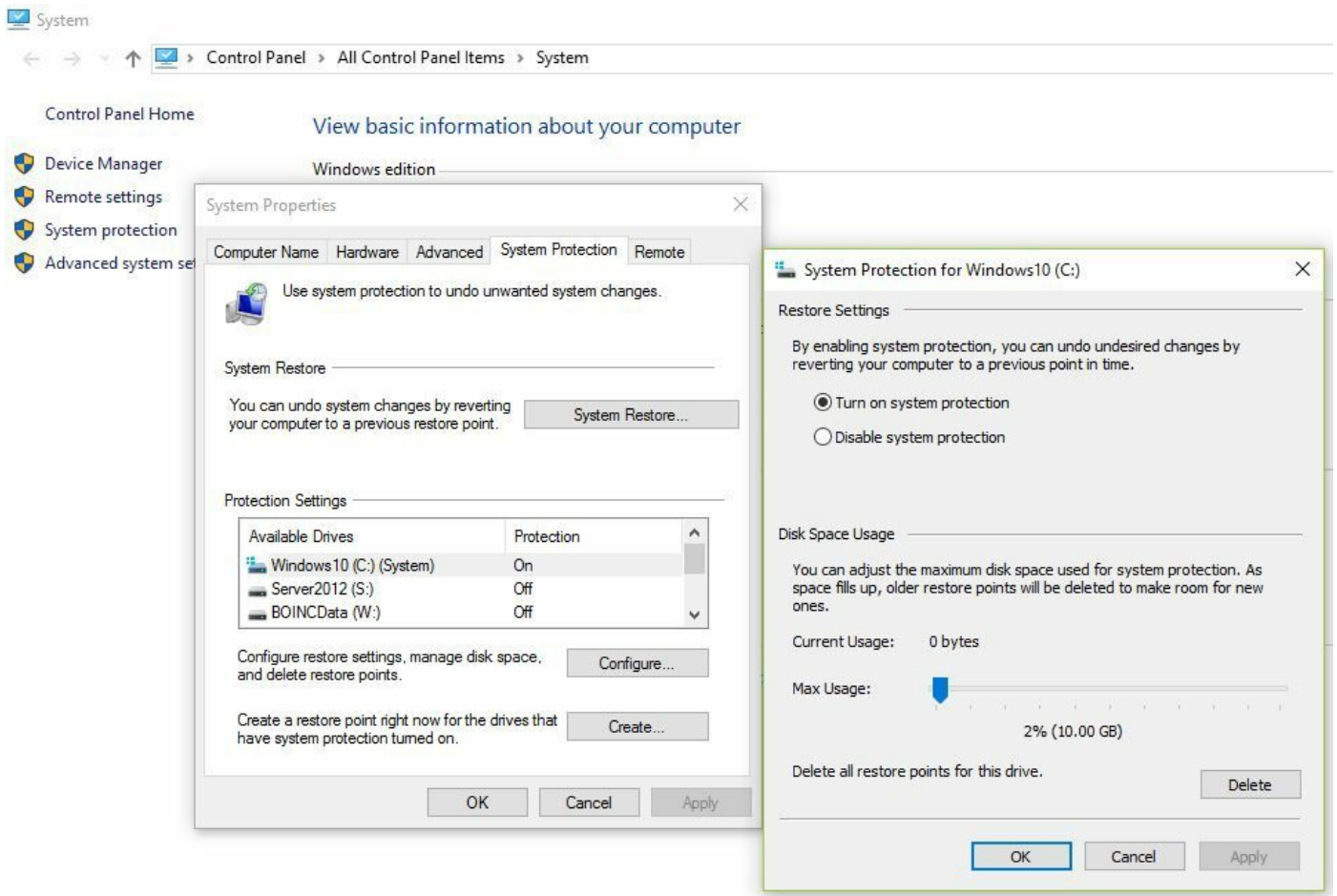






# System Restore

This tool is hidden within the advanced system settings pane. In order to set restore points you first need to allocate disk space for System Restore to use. Periodically checkpoints are taken when key system changes, such as an update or app has been installed and you can decide to roll back to one of these earlier saves if needed.

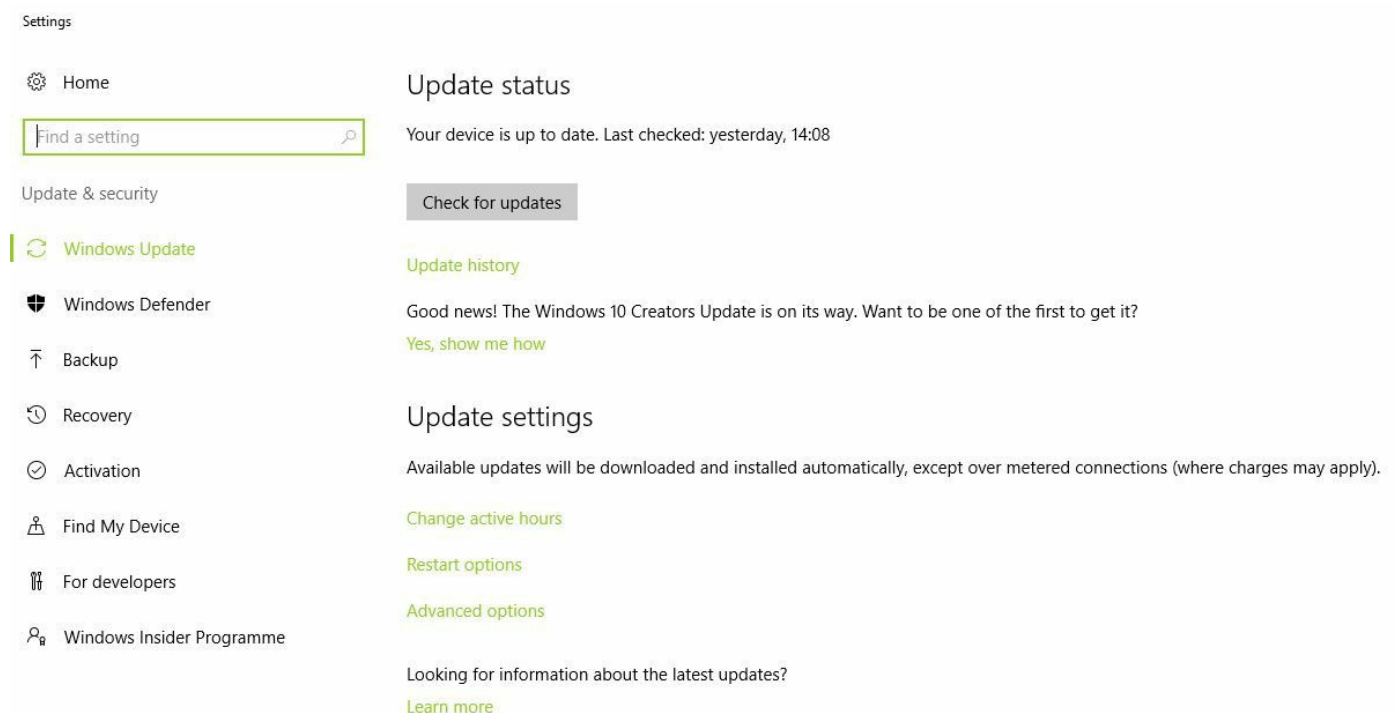




# Windows Update

The Windows Update settings has, for Windows 10 been moved from the Control Panel to the Settings cog. This new redesigned page allows you to turn on Updating, define if you are downloading updates only and manually installing them or completely automating the process. You can also list an update history showing all updates that have been already installed as well as the existing list to trigger a specific update to download or to install.

If you are on a Domain network and using a WSUS, the server will poll all domain machines and make a list of all of the updates needed. It will download one copy of the installer file and locate this on the WSUS server. Through a Group Policy we can define the downlink PCs (for example, client PCs) to instead gather their updates from the WSUS server and not direct from Microsoft's cloud. This way we only have to download the file once that then may be sent across our internal network to hundreds of PCs that need it.





# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Windows Administrative Tools:** <http://www.professormesser.com/free-a-plus-training/220-902/windows-administrative-tools/>
- **Windows Firewall with Advanced Security:** <http://www.professormesser.com/free-a-plus-training/220-902/windows-firewall-with-advanced-security/>
- **Using Windows System Configuration:** <http://www.professormesser.com/free-a-plus-training/220-902/using-windows-system-configuration/>
- **Using Windows Task Manager:** <http://www.professormesser.com/free-a-plus-training/220-902/using-windows-task-manager-2/>
- **Using Windows Disk Management:** <http://www.professormesser.com/free-a-plus-training/220-902/using-windows-disk-management/>
- **Windows Migration Tools:** <http://www.professormesser.com/free-a-plus-training/220-902/using-windows-disk-management/>
- **Windows System Utilities:** <http://www.professormesser.com/free-a-plus-training/220-902/windows-system-utilities/>





## 902.1.5 Given a scenario, use Windows Control Panel utilities

We have skirted around the fact that most of the settings you will need to configure are done through a central place--the Control Panel. On later systems, especially on Windows 10 the new Settings cog does not replace the Control Panel, but is designed for end-users to make low-level personalization changes, where the Control Panel is more powerful and far-reaching in how it can adapt and affect the OS. On a standard build of Windows 10, in icons view are 53 different panels affecting different aspects of the PC. In Category view, these have been themed and grouped together into eight groups.

In earlier versions of the CompTIA A+ exam there was a heavy focus on not only the breadcrumb trail but also the name of the panes. For example, Printers and Faxes (XP) was later labeled as Devices and Printers (7 upwards), but was called Printers (Vista). Whilst the functionality did not change you might find that some of the settings are also available through similar panes in the Settings cog for the end-users, however, in the cog pages you will be slightly limited as to what you can achieve.

At this stage Windows 10 is still new so not expected to be tested in the exam. Where there is a setting specific to Windows 10 these questions will only be introduced once the exam is established (so from 2017 onwards it is likely to see a Windows 10 question), but emphasis will be still on 8.1 as the last system to have researched before taking the exam, so W10 questions should also refer to an answer that is also applicable to earlier systems.



# Internet options

The internet options page is relatively unchanged since XP. It is used to define the homepage, also the connection settings and security lockdown of the Internet Explorer Browser. As Windows 8 upwards now use the new Edge browser as well, these settings will also apply to edge. Third-party browsers such as Chrome have their own equivalent settings page:

- **General:** This page is used to set the opening homepage triggered when a fresh IE session opens. You can also preset websites to also be loaded when IE opens and from here delete previous browsing history. The appearance of IE can also be set from this page (for example, fonts and colors used).
- **Security:** This page is used to set the different security profiles used depending on the resource you are trying to load. If you are loading an intranet (internal network) webpage hosted within your organization you will likely want a more relaxed security policy than if you were connecting to an Internet-based website. Trusted Sites are those sites you personally attest to being secure. These sites associated to this profile enjoy relaxed security settings. Restricted sites are those identified as potentially dangerous and so have been added to this profile that is typically set to very high security settings.
- **Privacy:** We can block certain sites from using cookies (text based information stored for convenience on the system. These may be form entries or passwords). We can decide if certain sites can view my physical location. Does a website show pop-up advertisements in a second window? We can block these from being seen with the pop-up blocker. Finally, the InPrivate Browsing mode does not record user data about the site you are visiting. It can be used often when you need to connect to a Federated account and don't want to use the cached user details. For example, you are using an email website such as `Outlook.Com`, but opening a normal browser session will use federated information and I will rejoin my existing session and see my email, but you want to log in with a second `Outlook.Com` account. How do you do this? By triggering InPrivate Browsing mode the session is clean, so you will be prompted to sign in. You can therefore effectively sign into two different accounts using two browser sessions.
- **Content:** User certificates are stored on the machine for authentication and encryption purposes. You can manage these through the content pane. The AutoComplete section defines if and to what extent autocomplete entries (suggestions for the rest of the text as you are typing in a field, if the key word has

already been typed) are set. The Feeds and Web Slices settings define how often to poll for interactive data updates from resources such as a financial index tracker or news feed.

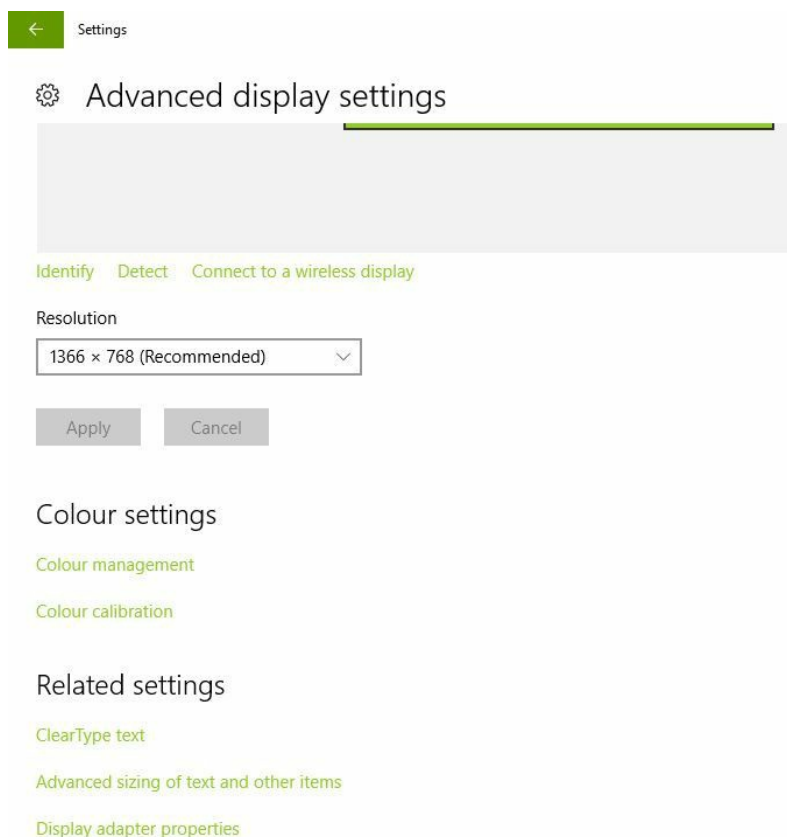
- **Connections:** This pane is used to set up new network connections enabling access to the internet. It originally was the page used to create modem profiles, or a VPN profile. If you are on a local network you do not need a dial-up profile at all. The LAN settings also are normally left black as internet options should not provide the configuration information to find the way to the gateway router - this is set by DHCP, or manually when a Static IP address is configured. It is common to lock the end-user out of this pane as the LAN button can be used to bypass a proxy server that may police the sites visited by the user. Usually this is blocked by Group Policy.
- **Programs:** This page defines the applications to be used to show HTML data for editing purposes. You can also define the web file types that are to be associated with IE.
- **Advanced:** Specific protocols allowed by IE, also more detailed security settings not found in the other pages are located here.



# Display/display settings

In the first section of this book, we looked in detail at the display concepts such as resolution, color depth, and the refresh rate. These can be set through the Display Options page that is easiest located by right-clicking the desktop in a blank area. On Windows 10 systems the options have been split into Display Settings (part of the settings cog). Here you can set the basic resolution, but through the advanced settings link a more detailed page allows you to set information we described previously.

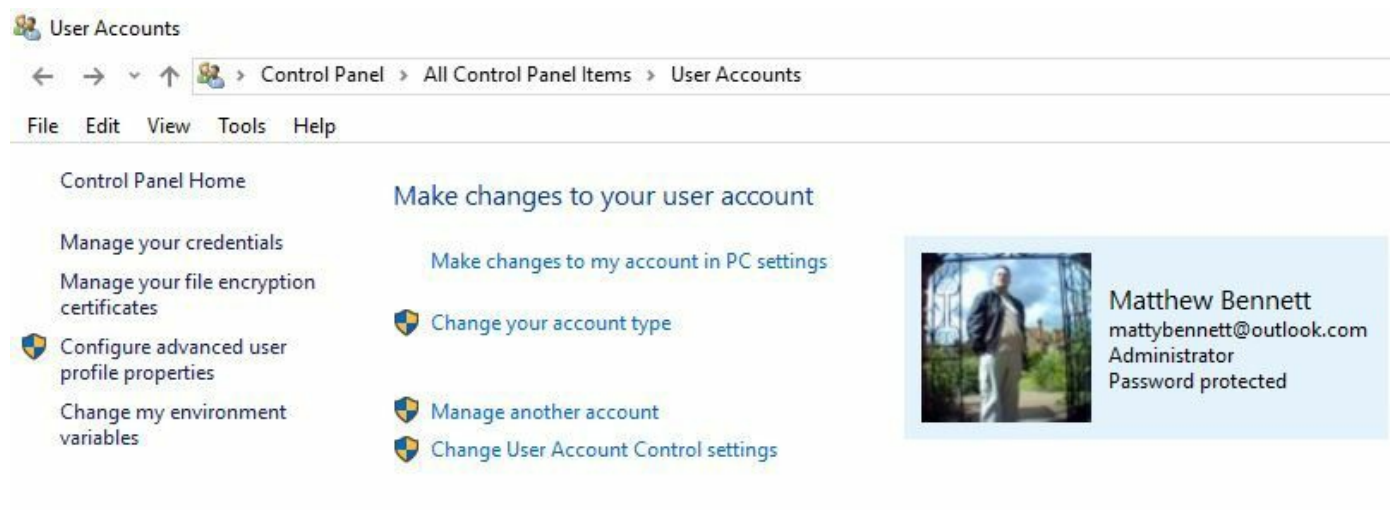
From the Control Panel, the Display page loads a generic page also allowing changing power plans, Brightness, the use of ClearType text to make the fonts easier to read, or to calibrate the color palette used by your monitor.





# User accounts

For Windows 10 User Accounts have now been limited and the connection of a Microsoft account to a local user account is now done through the Users pane in the settings cog. From here you can change your account type from a standard user to an administrator account (you need an administrator to confirm the change), manage other accounts if you have the permission to do so and set the User Account Control settings for this account to determine how often UAC will prompt you for elevation. I can also manage credentials attached to the user account such as certificates and keys stored in the Windows Vault (Credential Manager).






Settings


 Home





Accounts


 **Your info**

 Email & app accounts

 Sign-in options

 Access work or school

 Family & other people

 Sync your settings



**MATTHEW BENNETT**

mattybennett@outlook.com

Administrator


Billing info, family settings, subscriptions, security settings and more

[Manage my Microsoft account](#)

[Sign in with a local account instead](#)

Create your picture

 Camera

 Browse for one



# Folder options

Also accessible from This PC /File Explorer's View Ribbon and also called File Explorer Options (for this reason), this General page is used to control the interactivity with the system. From here we define if upon opening a new folder does it open in the same window, or a new window? Do we only need to single-click or double-click to start a file? Should we see recently used files and folders in the Quick Access list? From here we can also clear the file history.

On the View tab we can reset folder icons and define if hidden files and folders should be seen. We can show the filename extensions, show icons instead of thumbnails and also set these different view profiles for specific folders, or set generic settings for all folders.

The Search tab indicates the extent to which the system can index and search for files. We can exclude archives, define if we index at all and also include the filenames in the index.



# System

One of the first things I always do after a Vanilla-build is to visit this page. From here we can define the performance of the system. The Computer Name tab is used to set the computer name and also to join a workgroup or domain. The Hardware tab is used to quickly get to the Device Manager, also to determine if custom icons provided by the third-party manufacturers, or Windows' own icons are used for hardware. The Advanced page is used to access and set the performance of the PC at a granular level. You can define if the system resources should cater more for the best appearance, or performance, or a mixture. Equally on the Advanced tab you can favor programs running in the foreground, or background services. You can also set the Virtual Memory swap file size from here.



Microsoft recommends that the swap file should be 1.5 times the size of the physical RAM. You should keep the Min and Max values to the same as the initial size otherwise time is wasted re-sizing the swap file.

The Data Execution Prevention tab is used to protect files running in memory from attack by a virus. Essential Windows programs and services are protected by running in secured, reserved memory space. System Protection, as described earlier is used to enable System Restore and control the amount of disk space allocated to store the checkpoints. Finally, the Remote tab is used to enable remote management commands to this computer, also to allow Remote Desktop sessions to connect to this computer.



# Windows firewall

It is worth noting that the entry point into the basic Windows Firewall page is through Control Panel. From here you can then also access Windows Firewall with Advanced Security, which was covered earlier in the chapter.





# Power options

The Hibernate feature allows for all data stored in-memory to be saved as a binary file called `Hiberfil.sys`, located on the root of the `c:` disk. This file is loaded using a separate bootstrap upon powering the PC, returning the computer to the previous session exactly where it was caused to hibernate. Hibernation is often triggered either by pressing a 'sleep' key on the keyboard, or on a laptop by closing the lid. These triggering options can be set as part of the hibernation settings.

Separate Power plans are available for us to use. Balanced is a typical plan with standard settings where some hardware resources turn off after an amount of time has elapsed. The Power Saver plan is more energy efficient as switches off resources much quicker. High Performance is the opposite and does not throttle or shut down resources and is often used where energy consumption is not an issue.

Different to Hibernate, Sleep does shut down the PC placing it into a low-power state. The motherboard is receiving a residual energy to keep your data and settings in memory and the machine can be 'woken' bringing it quickly back to normal use. Sleep means different things, but in the Microsoft world Sleep is effectively the same as Standby, but if the power drops too low, or more than three hours have elapsed the system will hibernate and completely power down.



# Programs and features

In XP known as Add/Remove Programs this list shows all install applications on the PC. From here you can either install a new application (if you do not want to trigger from the installation media's setup file), refresh an existing application (for example, making changes to a suite of applications such as Microsoft Office), or uninstall an application that is no longer needed. From here you can also view all installed updates and turn on/off Windows features.

Programs and Features

Control Panel > All Control Panel Items > Programs and Features

Control Panel Home

Uninstall or change a program

View installed updates

Turn Windows features on or off

To uninstall a program, select it from the list and then click Uninstall, Change or Repair.

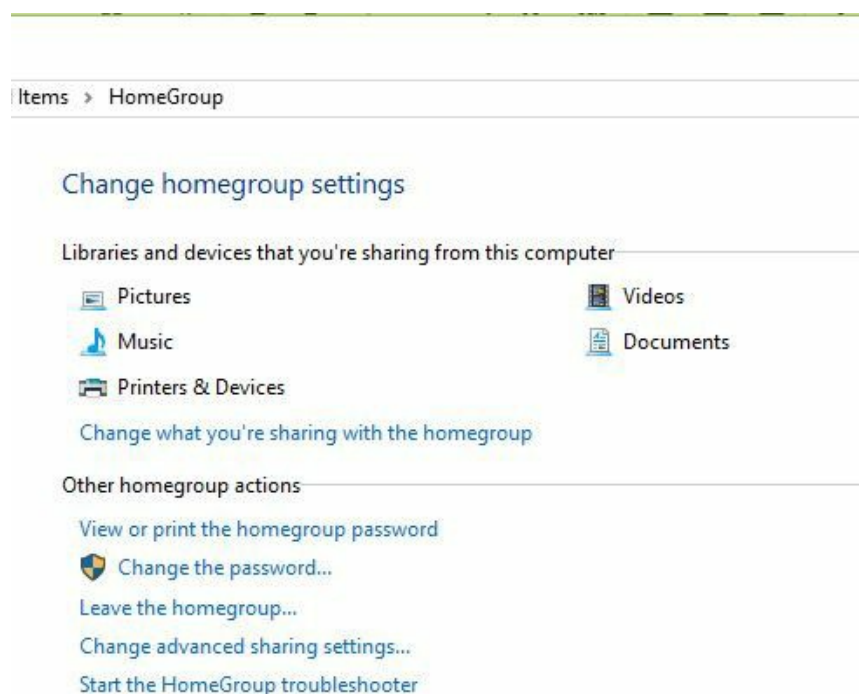
Organise

Name	Publisher	Installed On	Size	Version
7-Zip 16.02 (x64)	Igor Pavlov	26/09/2016	4.75 MB	16.02
Adobe Acrobat Reader DC	Adobe Systems Incorporated	11/07/2017	390 MB	17.009.20058
Adobe Connect 9 Add-in	Adobe Systems Incorporated	24/03/2017		11,9,979,355
Adobe Digital Editions 4.5	Adobe Systems Incorporated	08/05/2017	20.2 MB	4.5.4
Adobe Flash Player 23 NPAPI	Adobe Systems Incorporated	24/11/2016	19.2 MB	23.0.0.207
Adobe Photoshop CS	Adobe Systems, Inc.	16/08/2016	174 MB	CS
Android Studio	Google Inc.	20/07/2017		1.0
AnyTolSO	Crystalidea Software, Inc.	06/02/2016	21.3 MB	3.7.2
Apple Application Support (32-bit)	Apple Inc.	23/07/2017	172 MB	5.6
Apple Application Support (64-bit)	Apple Inc.	23/07/2017	192 MB	5.6
Apple Mobile Device Support	Apple Inc.	23/07/2017	48.4 MB	10.3.2.3
Apple Software Update	Apple Inc.	23/07/2017	5.41 MB	2.3.0.177
Audacity 2.1.2	Audacity Team	26/06/2017	62.6 MB	2.1.2
BBC iPlayer Downloads	BBC	26/06/2017	26.0 KB	1.14.2
Bethesda.net Launcher	Bethesda Softworks	13/01/2017	49.4 MB	1.0
Bonjour	Apple Inc.	08/06/2016	3.32 MB	3.1.0.1
Broadcom 802.11 Network Adapter	Broadcom Corporation	14/10/2016		
Broadcom 802.11 Wireless LAN Adapter	Broadcom Corporation	16/08/2016		6.223.215.14
Broadcom Bluetooth Drivers	Broadcom Corporation	14/10/2016	15.4 MB	12.0.1.850
Browser for SQL Server 2016	Microsoft Corporation	13/07/2016	13.9 MB	13.0.1601.5
Bullzip PDF Printer 3.0.0.352	Bullzip	10/09/2015	2.19 MB	
Cain & Abel 4.9.56		16/08/2016		
Camtasia Studio 8	TechSmith Corporation	09/06/2016	802 MB	8.6.0.2079
CCleaner	Piriform	20/07/2017	20.4 MB	5.32
Cisco WebEx Meetings for Internet Explorer	Cisco WebEx LLC	27/09/2015	20.6 MB	29.13.41.30001
Citrix Online Launcher	Citrix	10/11/2015	40.0 KB	1.0.362
CyberLink Power2Go 3.6	CyberLink Corp.	06/09/2015	87.6 MB	3.6.2.1307



# HomeGroup

Workgroups can have folder shares, but each PC is independent, which presents a problem--how can we centralize our shared folders and resources? This is possible with a HomeGroup that has been a feature available from Vista upwards. All PCs on the workgroup join a HomeGroup using a common password. Now you have access to a public folder in which you can store resources that need to be centrally available to all users across the group. The desktop page (in File Explorer, press the navigate up arrow to get to the desktop) contains a link to the HomeGroup. From the HomeGroup settings you can define the resources that can be shared.





# Devices and printers

As explained earlier, the Devices and Printers page is also available from Control Panel.





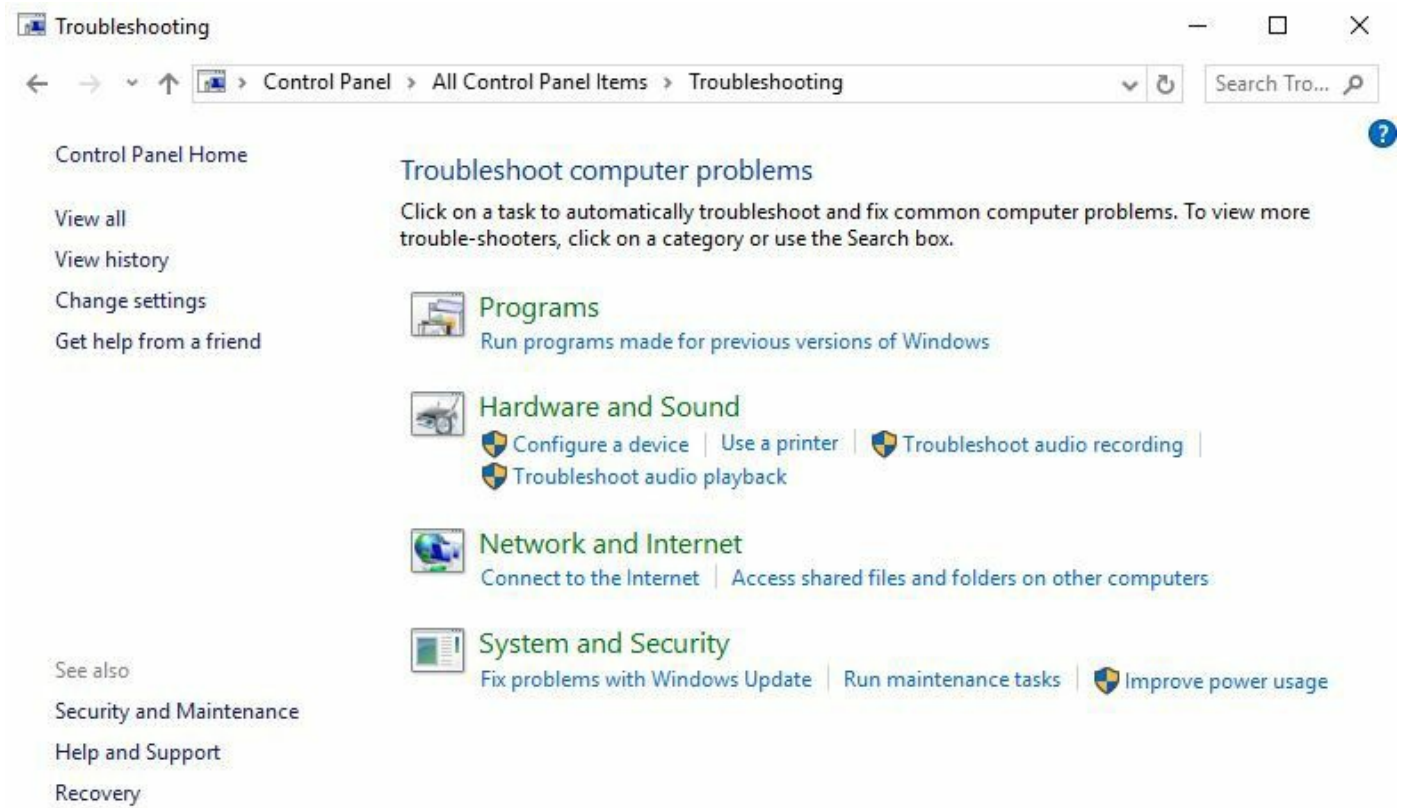
# Sound

The Sound page defined which recording and playback devices are used and on each one you can separately set the sound levels. You can reduce the sound of the playback devices when you are using the PC as a telephone, also set the audio sounds to use for different Windows actions (for example, alert bell, or the Shutdown Music).



# Troubleshooting

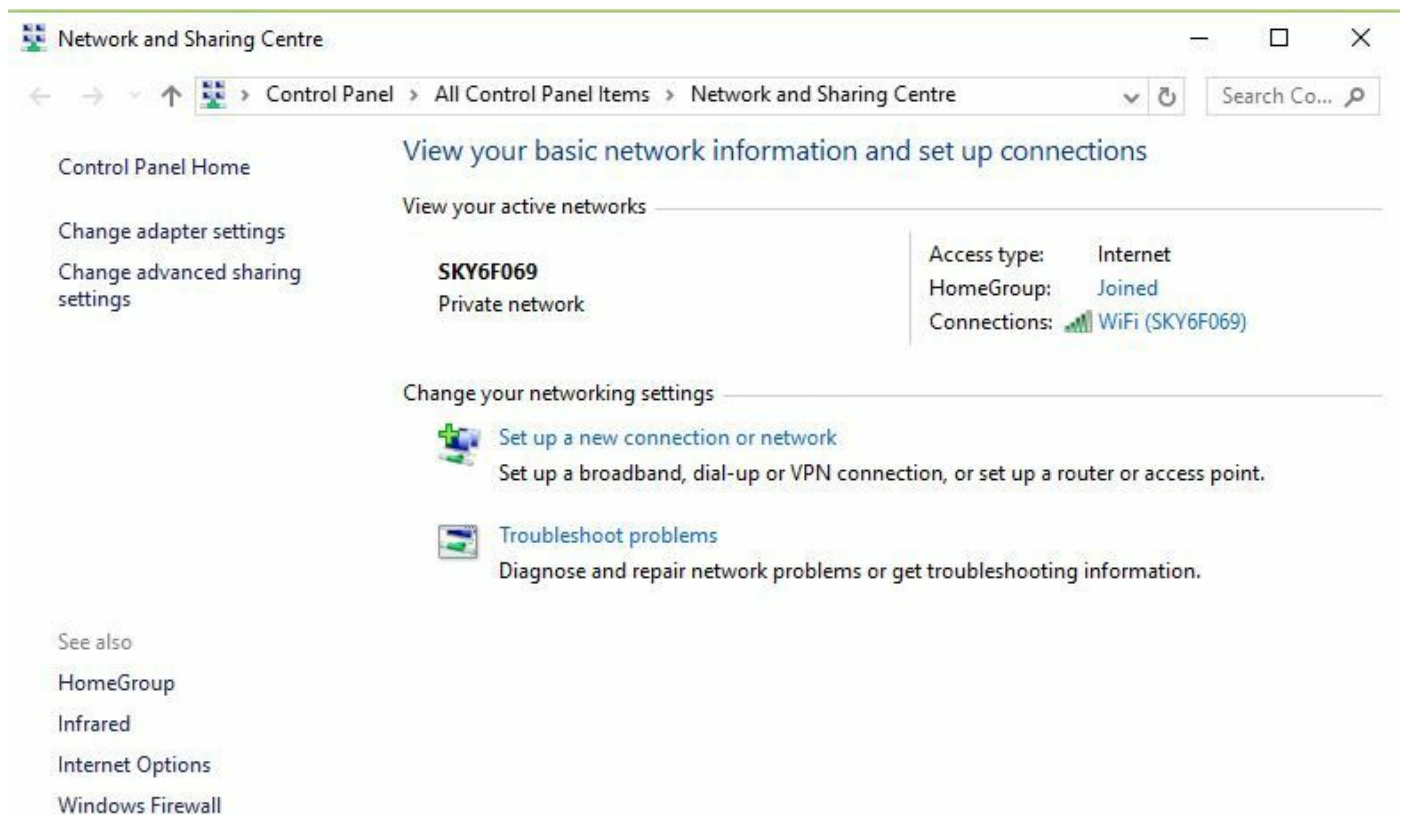
The Troubleshooting center is a list of over 20 different help wizards designed for endusers to fix basic problems with their system. These range from accessing Remote Assistance and sending an invitation for help, through to fixing display, sound, or networking issues.





# Network and Sharing Center

I'm keen to report as a Brit with a keen eye for English grammar that Windows 10 now labels this page correctly as Network and Sharing Centre. This page is used to show the active network I am currently connected to and where you are part of a network you can use an LLTP-created network map listing all devices in the local neighborhood that are also part of the same network. From here you can also create a new network connection, such as a dial-up connection to and ISP, or a VPN tunnel. This page also links to the Networking group of troubleshooting wizards, but more helpfully you can use this page as a starting point to access the Network Adapters page. This is frequently used to set IP addresses to network devices. Finally, the advanced sharing page, also accessible from here, enables Network Discovery and File and Printer Sharing. This is enabled per network profile separately.





# Device Manager

Finally, Device Manager enables us to view the current hardware profile of the PC, as detailed earlier in the 901 section of this book.





# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **The Windows Control Panel:** <http://www.professormesser.com/free-a-plus-training/220-902/the-windows-control-panel-2/>



## 902.1.6 Given a scenario, install and configure Windows networking on a client/desktop

This section of the chapter is not describing, for example, what a Workgroup is, rather trying to determine when you might need one. We look at a typical usage scenario and describe the benefits it will provide:

- **HomeGroup versus Workgroup:** A Workgroup is typically used on a network that may still have XP machines, or no need of a centralized folder storage solution. It may be that one computer has been designated a file server and separate shares to that file server are also set up on the existing client PCs. In this scenario a HomeGroup is not necessary.
- **Domain setup:** Any more than 10 PCs and a Workgroup starts to become unmanageable, at which point you will want to decide instead to centralize access control as well as resources. Typically the DHCP server centralizes IP addressing, DNS centralizes network resource lookups, the Domain Controller centralizes authentication, a Print servers centralizes management of all of the printers across the site, and a File Server is used to centralize all user documents to make backups easier as well as keeping shared folders in a central area.
- **Network shares/administrative shares/mapping drives:** A drive is mapped to volume letter. This is a local resource because it is local to the PC. Each PC's first hard disk contains a partition formatted as a volume known as c:. Therefore, everybody's c: drive is different and unique to their computer. A Network share is a shared folder available on a specific computer. To access it we use a Network Share written using a **Universal Naming Convention (UNC)** system such as: \\<domain>\<Computer Name>\<Share name>. For example: \\server01\myshare

A drive can be mapped against a drive letter, or additional disk space on another hard disk can be added to an existing volume by mapping it to an empty folder within the existing volume's structure (referred to as a mount point). This can either be done through File Explorer or more commonly through Disk Management or the command tool `DISKPART`.

By default, every volume letter is automatically shared. This is a hidden share, also known as the administrative share. These do not appear in the network list

on the Network page. Also, if you manually share a folder and add a \$ at the end of the share name this will also hide the share:

- **Printer sharing versus network printer mapping:** If a printer is shared, the drivers to operate it are local to the printer--the print device is locally attached to the PC and this PC has to be left switched on to be able to cater for other network PCs who may want to use the print device through the shared printer. By centralizing this role we attach the print device, usually via a network cable to a print server that serves the entire network. The Print server holds two roles - it manages the print queues for all print devices on the network it looks after; also, it stores the driver files needed for the print server to operate and render print jobs. Where the printer has been set to render the print job on the local PC instead, the print server is used as a repository to store and to send out client-side drivers as needed. The print server is typically a 64-bit machine, so often we have to store both the 32 and 64-bit versions of the printer driver to support older client systems.
- **Establish networking connections:** Network connectivity is not given. Standalone PCs may request an IP address if a DHCP server is present on the subnet. If it is not we will have to access the Network Adapters page and set the IP settings manually. We establish a network connection as follows:
  1. In Command Prompt run `IPCONFIG /ALL` to determine if an IP address for the network device has already been configured (in this example, we will imagine that we are setting up a network interface card).
  2. If a DHCP server is available on the network run `IPCONFIG /RENEW` to trigger the DORA process and obtain an IP address.
  3. If you need to set the IP address up manually, make a note of the default gateway IP address and if possible the subnet mask in use.
  4. In Network Adapters, select the NIC to adjust and on the properties page select IPv4 properties. Set the IP address to the same subnet range as the rest of the subnet and add a final octet number that you know is not in use on the network. Set the subnet mask so that it matches the subnet (you may need to view the settings of another known good PC on the network first) and set the default gateway for the router to be same as is in use. Set the DNS Server's IP address to match that on the known good.
  5. Upon pressing OK the network adapter status will change and after a few seconds should report the correct network name. Alternatively, an `IPCONFIG` will show the correct settings. Test accessibility by pinging another known good PC on the subnet, then an IP address out of the subnet. Test internet

connectivity by pinging a known good website by its URL that also proves that DNS resolution is taking place.

The Network and Sharing Center can be used to set up various connections, from dial-up, wired, and wireless connections also to cellular tethering. With Windows 8 and higher a separate Wireless pane appears on the right of the desktop that shows the result of a wireless network scan. You can then connect to these devices. If a VPN profile has been created, this will also appear in the same pane. Where you have decided to tether to a mobile phone and use it as an access point, sharing its Wi-Fi or mobile data with your laptop across a USB cable the pane will show a new network. This will be a PAN network of your laptop and the mobile phone only.

By means of a recap, here is a reminder of some of the other key elements it would be worth noting:

- **Proxy settings:** Within Internet Options, we can bypass or set the IP address of the proxy server. The Proxy server keeps a cached copy of a website once it has been visited. Other users see the cached copy of the webpage (where the page is a static HTML page). Proxy servers are also used to screen and monitor internet access and from here you can create and use a security list banning certain websites from being accessible on the network. Remote Desktop Connection - MSTSC provides a connection window allowing us to connect to a remote PC. Remote Assistance - Different to MSTSC, a shared invitation file is sent to another person who will then connect remotely to your session. You share the session between both parties who can both control the device. Home versus work versus public network settings - As discussed earlier and now referred to as Public, Private and Domain, these security setting profiles are used to determine the level of security used depending on which network your device is connected to.



# Firewall settings

The Advanced Security screen can be used to also set firewall exceptions, allowing certain program access to a specific port, once the program is running. Key applications and windows services can be allowed access through the firewall and this can be set differently for each profile. More detailed configuration of the firewall is possible through the creation of Firewall Rules, using the Advanced Security page.

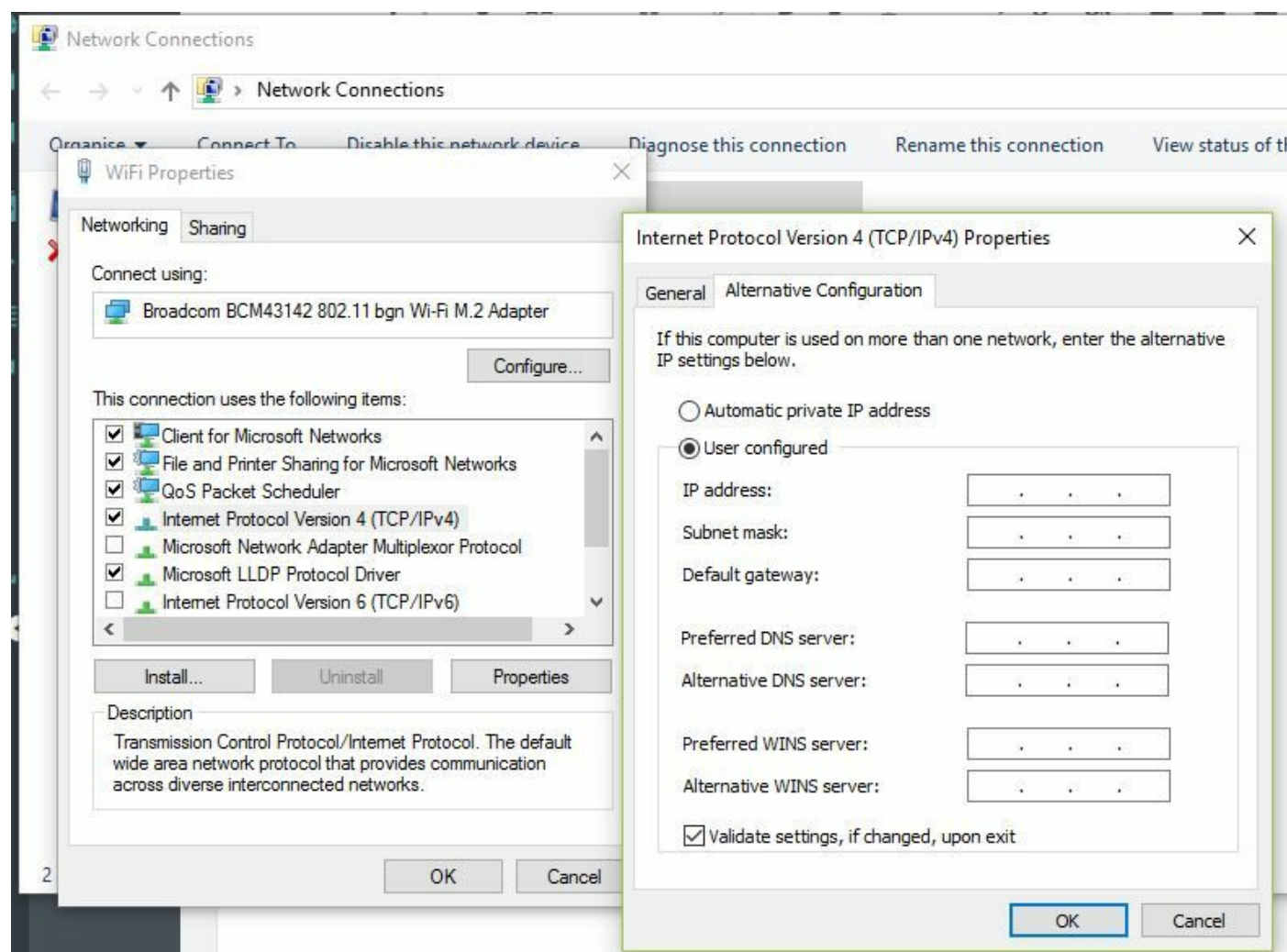
Enabling/disabling Windows firewall--It is highly recommended that you never disable the firewall. The firewall does a very important job to screen data entering and leaving your computer. However, the firewall page does have an option to switch off the firewall completely, but this is tied to whichever specific profile you are using.





# Configuring an alternative IP address in Windows

This mainly applies to a laptop, which is designed to be used at various locations. The typical setting for a NIC would be to allow DHCP to set the IP address automatically. However, when you are away from the network, such as if you decide to use your laptop at home it is very likely that the IP configuration at home will be different to your office network. Windows provides an Alternate Configuration tab where you can set a second set of IP addresses to use when not joined to the domain as shown in the following screenshot:





# Network card properties

Within Device Manager, on the NIC properties page you can set properties specific to the NIC common properties are:

- Half duplex/full duplex/auto: The term Duplex refers to the fact that data can travel from PC A to PC B, but also PC B can also use the same cable to send to PC A. Bandwidth will either be shared so that half of the throughput is used to send and the other half to receive. With Half Duplex all of the throughput is sent for 1-way traffic. The other device has to wait to then reverse the direction and send using full throughput. With the automatic setting devices will decide amongst themselves whether to use Half or Full duplex.
- Speed: TCP never sends a file using the faster speed possible. The two end devices agree on a speed which works for both parties and sends at this slower speed. Across the session the speed is increased until the fastest possible speed is used. FireWire on the other hand always sends at the fastest possible speed. The speed at which the network card will operate can be set here (typically 1Gb/s)
- Wake-on-LAN: If a PC is in sleep mode residual power is also going to the NIC. A Magic Packet can send a low-level command instruction to wake up the PC from sleep mode, returning it to normal power where the PC can then be used. This is often used by remoting staff needing to access a service on the network PC.
- QoS: We also discussed **Quality of Service (QoS)** in the 901 section of this book. Video streaming is often susceptible to environmental conditions that can affect the best speed to send the stream at. QoS keeps the line connected by throttling the speed. By doing this, although there is a drop in quality, the line stays open. Added to this video streaming data traffic is prioritized by the PC - other network traffic is asked to wait.
- BIOS (on-board NIC): Where the NIC is integrated into the motherboard its speed can also be set in the BIOS. Also you can switch off the integrated NIC entirely via the BIOS. This is only done when you are replacing the on-board NIC for a better one connecting through the PCI sockets.



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Windows HomeGroup, Workgroups, and Domains:** <http://www.professormesser.com/free-a-plus-training/220-902/windows-homegroup-2/>
- **Windows Network Technologies:** <http://www.professormesser.com/free-a-plus-training/220-902/windows-network-technologies-2/>
- **Establishing Windows Network Connections:** <http://www.professormesser.com/free-a-plus-training/220-902/establishing-windows-network-connections-2/>
- **Configuring Windows Firewall:** <http://www.professormesser.com/free-a-plus-training/220-902/configuring-windows-firewall-2/>
- **Windows IP Address Configuration:** <http://www.professormesser.com/free-a-plus-training/220-902/windows-ip-address-configuration-2/>
- **Configuring Network Adapter Properties:** <http://www.professormesser.com/free-a-plus-training/220-902/configuring-network-adapter-properties-2/>



## **902.1.7 Perform common preventive maintenance procedures using the appropriate Windows OS tools**

Up to this point we have described specific components and how to configure them, but various technicians will set things up indifferent ways based on their own experiences and intuition. Vendors however may have very good reasons why a device has to be configured in a certain way and this rationale is not always obvious. We are going to look at preventative maintenance we can take to ensure that the system stays in good condition.





# Best practices

As a technician, your role, as well as fixing faults is also to ensure that vendor advice is followed so that the systems work at optimal levels and error-free. IT systems do not work well cross-vendor and this can be a problem for IT teams as companies buy into software and platforms based on their need and most often do not stick with one vendor, or provider. This leads to complications caused by the inability of the systems to integrate. Work has been done here to use universal languages such as XML. This section will provide vendor guidance for common tasks.



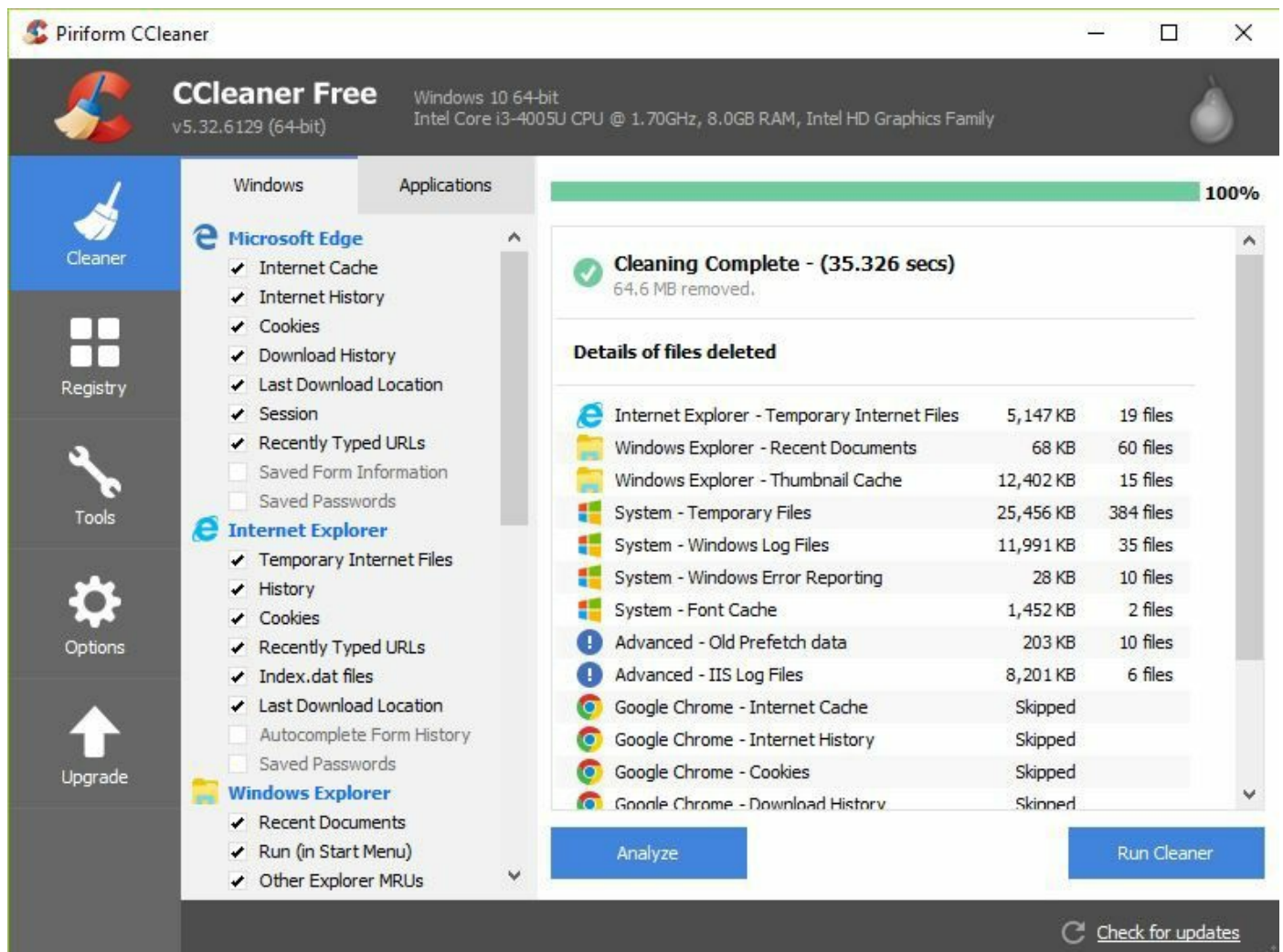
# Scheduled backups

In an earlier section I explained a company who had a member of staff responsible for adding a backup tape to a server, but actually never triggered the backup to run. In the 901 section of the book we looked at how often and the type of backup you should take to protect data. From a physical perspective we talked about using several tapes and regularly replacing them (Grandfather-Father-Son), also how we should equally use the tapes to avoid over-wearing one tape (Towers of Hanoi table). We also discussed a backup strategy (for example, Normal backup with following Differential backups) to use which is the best for your particular scenario answering the question "Which is most important for you? The time taken to backup, or the time taken to restore data onto the system?" Finally, we spoke about using Windows own Backup tool and that users of this server had to be members of the AD Backup Operators group.



# Scheduled disk maintenance

Each disk should be regularly checked for physical damage by using the `CHKDSK /F` command unless your disk is part of a storage space in which case it will be checked by Server Manager automatically. Disk performance can degrade as the file structure becomes fragmented. Periods of intense installing, or uninstalling can also cause massive gaps in the volume structure and these are also good times to then defrag the PC. Before Disk Checks or Defragmenting, you should run a sweep to clean any temporary files and unwanted junk files that are part of old installations, or user profiles but are no longer needed. Although Windows can do this from File Explorer I personally use a third-party tool equally as efficient called PiriformCCleaner (<https://www.piriform.com/ccleaner>). It is free, quick, and reliable.







# Windows updates

It is absolutely vital to keep the PC's core system files up to date. This is done through Windows Update on the home PC, but on a domain best practice is for the Network Manager to test each update on a test workbench not connected to the domain first, then if they are happy to, they approve the update on the WSUS server. The WSUS server only sends across the network updates that have been approved.





# Patch management

Typically a company will not upgrade their Operating Systems to a new release until it has proven to be stable and reliable. This is usually after the release of Service Pack 1.



# Driver/firmware updates

Here, the advice is only to use approved drivers located on the Windows Update server, or from the manufacturer's website. Secondly, ensure that the driver is digitally signed.



# Antivirus/anti-malware updates

Windows Defender regularly prompts the user to ensure that their antivirus database is up to date before running a scan. Action Centre will provide a pop-up message in the corner of the desktop periodically to ensure that end users take responsibility for ensuring that their PCs are kept up to date. Where you are connected to a Domain with a System Health Validation / Remediation server if the PC is considered to be unhealthy it will drop out of scope by receiving a quarantine IP address so that it cannot infect the other computers on the network.



# Tools

In order to implement these maintenance tasks we use:

- **Backup:** Windows Backup is a feature of Server 2012. Once installed users would have to be Server Operators and members of the Backup Operators group.
- **System restore:** Restore points need to be enabled and an amount of disk space allocated to the System Restore service so that checkpoints can be taken. Checkpoints are automatically taken at key events such as a major install or driver installation, but you can through an AD Group Policy set checkpoints to be taken at specific times.
- **Recovery image:** Once the Vanilla-build has been configured and the system is at its optimal condition a Recovery Image can be captured and saved to an external device for use in an emergency. In Windows 10, from the settings cog, go to the recovery page where you can prompt to reboot the PC directly into the Advanced Startup menu. From this menu go to Troubleshoot, Advanced Options, and then choose System image recovery where you can specify an external disk to save the captured image.
- **Disk maintenance utilities:** Although third-party tools are also available we referenced CHKDSK, DISKPART, Disk Management, also the built in cleanup and disk check tools available from File Explorer by selecting a volume's properties. On the Tools tab are the error checking and optimize tools.





# Exam questions

1. A user needs to access a file stored yesterday. They have worked on the file since then but the new changes to the file are not what they wanted. They want to revert to the previous version stored yesterday. What feature allows them to do this?
  - Answer:
2. After checking a laptops hardware you discover that it has only just enough RAM to run the main operating system and very little else for user data, or for applications to run. Your laptop is already fitted with the most amount of RAM the motherboard can handle. Despite this, you still need to extend the amount of RAM. How is this possible?
  - Answer:
3. What are the firewall profiles available on Windows 8.1 and where are they used?
  - Answer:
4. What application is used to create an unattended installation file used with your installer disc to automate the process of installation?
  - Answer:
5. What is the difference between Refresh and Reset?
  - Answer:
6. I want to copy a website stored on my web server to another web server. The site consists of thousands of GIFs and JavaScript files making the file transfer take a long time. Transferring often fails due to the amount of files, also the network connection is not stable. What command-line tool can I use to reliably copy the entire website?
  - Answer:
7. I have just applied a GPO to an Active Directory group. The policy has been sent across the network to all client PCs. The GPO is a User policy affecting the Sales group. I have logged on to a Sales PC and want to check to see that the policy has been applied without logging on as a member of the Sales group. How can I achieve this?
  - Answer:
8. I have an old Audio codec needed by a legacy program. There is no installer file, simply a DLL file. How do I get Windows to be able to use the DLL?
  - Answer:
9. I am suffering a performance drop. The system is taking far longer than usual to access user files. What can I do to remedy this?
  - Answer:

10. I often take my laptop home and want to connect it to my home network. When I am in the office I receive my IP address by DHCP, but do not have this capability at home as IP addresses are statically assigned. How can I connect to both networks?
- Answer:



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Windows Preventive Maintenance Best Practices:** <http://www.professormesser.com/free-a-plus-training/220-902/windows-preventive-maintenance-best-practices/>
- **Windows Preventive Maintenance Tools:** <http://www.professormesser.com/free-a-plus-training/220-902/windows-preventive-maintenance-tools/>



# Summary

This section is one of the most important in the 902 exam. If I can give you any advice it is to be absolutely comfortable with the Windows Operating Systems from Vista onwards first, and then learn how Apple and Linux have equivalent tools.

In earlier versions of the test, CompTIA was known for being very Microsoft heavy despite the fact that the exam is vendor agnostic. The occasional reference to Linux was with questions referencing the `IFCONFIG` command and Apple was only really mentioned in-passing by referring to an iPhone, or to say that an action was also possible in macOS, but not really to explain how. With this version of the exam all of this has changed. While Microsoft is still important, scenarios now explicitly state how things are done in the other systems. You will need to know the limitations of, for example, Apple systems - you might be given a scenario to connect an iPhone to a Wi-Fi access point, or might need to read a network diagram and also check the network IP settings across several devices to find the problem on a network.

Cisco and Netgear also feature more extensively than they used to. Expect to see Netgear routers referenced as SOHO or Home routers and Cisco for Enterprise networks. It would be advisable to take a look at the user interfaces for these, especially Netgear and a link to online simulations of Netgear routers will be available to you in the next chapter.

This chapter looked at the different features of the later Windows systems from Vista to Windows 8.1. I also reference in-passing through the section of this course Windows 10 as it is built on the same architecture as Windows 8.1, also because I am using Windows 10 here, so it is easy for me to grab a screenshot to show you and the interface is the same on 8.1 for most things, but also to future proof this book as Windows 10 will feature in the exam shortly.

We then learned how the system boots, looking at boot partitions and partitioning tables used to structure the disk. We considered formatting these partitions in different ways and the benefits each formatting type gives us, also where we would expect to use them. We also considered from the perspective of booting the system how to access the Boot Menu and where this menu is stored, also where the system files are stored. I also referenced how to boot across a network, even to deploy an image from across the network.

We then looked at a variety of Command-Line tools used to perform system and file changes before then looking at some depth at a variety of GUI tools that form the core system. Finally, we covered GUI tools that form the system control panel.

I then gave you a series of scenarios, explaining how to access network resources across the network. We considered different forms of network (for example, Workgroup), plus network tools for support, or for monitoring. I then also mentioned characteristics of the NIC itself, such as the ability to Wake-on-LAN using a magic packet.

Finally, we looked at best practices concerning PC OS maintenance, covering driver and patch management, also taking backups and how to manage, tidy, or recover the volume.





# Other Operating Systems and Technologies (902.2)

Any projects you create will have to cater not only for Microsoft systems but other systems as well. I learned Microsoft systems first and then this gave me a context for the others, which are, in fact, very similar. In this section, we are going to identify some of the common features of both macOS and Linux.



## 902.2.1 Identifying common features and functionalities of the macOS and Linux operating systems

To help you learn how to use Linux, it would be a good idea to have your own online lab. Download an ISO of Linux and install this onto a virtual machine in Hyper-V, or, using an Azure account, you can create a pre-installed Linux distro within a matter of minutes (for example, the latest ISO of Ubuntu is available at <https://www.ubuntu.com/download/desktop>).



As a useful starting point, try is an interactive tour of Ubuntu, available at: <http://tour.ubuntu.com>.

As I mentioned in the e-networking chapter summary, network devices such as Cisco switches/routers (for more details, go to <https://www.cisco.com/c/en/us/products/routers/index.html?stickynav=2>) and NetGear or LinkSys routers, will feature in your exam, possibly also in the simulations. NetGear routers are available (from a French version of the website) from <http://firmware.netgear-forum.com/index.php?act=interface> and Linksys routers are available from <http://ui.linksys.com/>.



# Best practice techniques with Apple systems

As with any system, it is best practice to keep the system running well and for data to be backed up. Apple has its own backup utility in OS X called **Time Machine**. This automatically backs up data every hour and keeps the last 24 hours of backup data, daily. As long as you have allocated sufficient disk space, Time Machine also backs up a month's worth of data. It deletes backup data starting with the oldest first. When Time Machine is first started, a wizard will ask you which drive to use to perform the backups.

Apple, unlike other systems, is designed for everyday technology users, and just works. With this in mind, tasks such as disk maintenance rarely need to be run manually because the system is regularly and automatically performing disk maintenance already. The disk utility is a central point to mount disks, perform first aid on a disk (equivalent to Microsoft's disk checking utility), erase a disk, unmount a disk, or view disk information, such as the number, size, and type of partitions located on the disk.

OS X updates can be found in one key location. Updates for both the OS (patch management) and installed apps can be found in the Updates page within the App Store. Users can set updates to install automatically, or they can be triggered manually.

The Apple end user is rarely interested in the actual hardware makeup of the device because the Apple PC is purchased as a complete device in-store. Should anything go wrong with it, Apple technicians in the store will assist you, or make configuration changes for you in the same way that if I buy a car new from a Honda dealership, and if I notice something is not right with the car, it will be checked and adjustments will be made under its warranty. I do not need to know about the car's mechanics to be able to use the product. Apple's concept is that the PC is a product; a commodity.

Apple OS X does provide a system information list similar to the SYSINFO32 report in Windows, which provides detailed information about the hardware make, model, software versions, and also the driver and firmware versions installed on the device. Unlike Device Manager in Windows, the report is read-only and cannot be used to make changes to the drivers or update the drivers from this tool.

OS X does not ship with an antivirus solution at all. You need to consider purchasing a

third-party solution to protect your system. Please do not take the view that viruses never hit Linux or Apple systems--they absolutely do.





# Tools

Time Machine is very simple to use. The utility basically has an on/off button and a settings button to define how much disk space to give to the Time Machine backup and where the backup will be stored. Again, when Time Machine is first run, you will be prompted to select which disk to use for backups.

Time Machine can also take snapshots of the local drive. You can then enter the snapshot (think of it as an archive file) and recover any files you need, copying them back to their original location.

To explain, a Linux distribution (distros) is a collection of software and a specific version of the Linux core code. Each distro is marketed with a brand name and some are focused towards certain audiences. For example, Debian is a light Linux footprint that will work on ARM processors, such as phones, or a Raspberry Pi. **Edubuntu** is the scaled-down image of the main Ubuntu desktop system. Edubuntu was designed for school users. Xubuntu is a light version of Ubuntu with a stripped-down list of drivers in the kernel. Linux Mint has a UI which is similar in design to Windows XP, so is designed to attract Microsoft users.

One backup tool used across all distros is **Tar**. Tar was originally designed to be a **tape archive** controller and creates an archive file known as a **Tarball**. **Rsync** is also used to copy folders between computers. Both Tar and Rsync can be scheduled.

Filesystem maintenance is automatic. The disk filesystem is checked periodically after a few reboots. If a file has been added to the root structure, then the disk is automatically checked on the next reboot. To force a recheck, use the command `sudo touch /forcefsck`.

The `sudo` command stands for **super user do** and is the equivalent of a Run As Administrator option in Windows.

One possible manual job you may need to do periodically will be to clear the log files folder. This can be found in `/var/log`.

Operating system and application updates use different tools that vary based on the distro you are using. Common tools available are `apt-get` (for example, on Debian systems) or `yum`. There are also graphical catalogues, such as the Ubuntu software center, which is similar to Apple's App Store.

The main difference with Linux is that most of the device drivers used are common ones that already form part of the core operating system code (referred to as the Kernel). Additional drivers can be installed, and may need to be installed if no equivalent driver is in the Kernel, but most hardware just works as Kernel-mode drivers are usually very good for running most standard hardware you would expect to find in the system. Additional drivers are usually installed through the Software & Updates page.

Linux distros do not typically ship with antivirus software, so you will need to install third-party ones, as with Apple. There are a variety of open-source antivirus applications on the market, and if a provider makes an antivirus application for Microsoft systems, expect them to also supply a Linux variant. Once installed, ensure that the virus definition files are up to date and that you are allowing the application to perform real-time scanning.

The built-in disk utility discussed earlier also allows you to capture an image of an entire hard drive, creating an Apple disk image (a DMG file). This file can be mounted on any macOS X system, and is a much easier method of taking a system image than any Microsoft provides, which, because of its copy protection, locks the image to the hardware profile and license key.

With disk utility you can mount, unmount, create, resize, and move volumes, as you would expect.

Additional functionality is available with the Terminal window. Here you can run scripts, manage files, configure applications, and run system commands. The Terminal can be found using the Finder tool (akin to Windows' Start menu) | Utilities.

As with Windows systems, you can have a virtual desktop of several virtual monitors and swap between them. You can also share your screen with another output port, similar to the Project tool in Windows. However, one advancement is that the screen sharing for Linux also supports sharing across a **Virtual Network Connection** (for example, PuTTY, or TightVNC), so you can stream your screen as a remote desktop window. To find which devices are using screen sharing, you can look in the Finder.

In Windows Task Manager, you can select troublesome applications that have stopped responding and end the task. The Linux equivalent, Force Quit, can be used by pressing the command, option, and escape keys at the same time, or go to the dock application, scroll to the application you want to close, right-click with the mouse, and select Force Quit.





# Features of Apple systems

As there are several distributions, there are often several apps and command tools that do the same job. You might therefore find, for example, that you have various different backup, or app installation tools loaded, each giving you slightly different access. You might find, for example, that if you want to install the Python command language, that `apt-get` might work on some Linux distros, whereas in other cases it may be easier to install from a Tarball, or from the Ubuntu software center.

Mission Control (formerly Exposé), for Apple users, is an app that lets you view all open windows with one key press. Overlapping windows can also be tiled. This is similar to the Alt + Tab Aero feature in Windows systems. To use it, double-tap the mouse to open the Dock/Launchpad. Press the Mission Control key on the keyboard, or Ctrl and the up arrow.



Apple's password management solution not only stores user passwords for websites and applications, but also credit card information. This is linked to your iCloud account. It works with iOS 7.0.3 or OS X and later systems. It is analogous to the Windows vault; however, sensitive data is stored in an encrypted format and is accessible across all of your Apple devices linked to your iCloud account.

A device has to be approved by the user to support Keychain. When you add a new device, one of the other devices already linked to iCloud and using Keychain will receive a request to approve the device before it is added.

To set up Keychain on OS X, perform the following steps:

1. Choose Apple Menu (press the Apple button on the keyboard) | System Preferences and then click iCloud.
2. Select Keychain. If you want to, you can set a passcode to unlock your screen after sleep or after the screen saver begins.
3. Enter your Apple ID and password.
4. Follow the onscreen instructions at: <https://support.apple.com/en-gb/HT204085>.
  - **Spotlight:** Similar to a Windows search, the engine performs a search for files using an index. You can find user documents, music, images, videos, and even system preferences. Keyword searches will also check recently viewed web pages stored in the cache as well as bookmarked pages. Word definitions are also provided with information referenced from the New Oxford American Dictionary. As with Google's search, Spotlight will also perform calculations for you if you enter an equation into the search field:



- **iCloud:** An iCloud account is not only a cloud-based storage solution, but an extremely secure one. It can be used to share information between all of your Apple devices, also keeping those devices synchronized to each other by sharing contact information, email, calendar information, reminders, tasks, and iTunes purchases. It is a central storage point for all of your personal information and is free.

It is analogous to a Microsoft account and how it gives you access to OneDrive, as well as basic Office functionality, a shared calendar, and so on. The major difference is that the synchronization data sent to the device from the iCloud is heavily encrypted, and considered to be secure.

The iCloud account can be viewed on an iOS device by going first to the settings pane, and then tapping iCloud. For a PC, you will need to install the iCloud Control Panel for Windows. For a Mac, go to the System Preferences page from the Apple menu, and then click iCloud.



You can register for an iCloud account at <https://www.apple.com/uk/icloud/setup/mac.html>.



- **Gestures:** The Apple system supports multitouch gesture control, which allows you to use two fingers to perform actions.
  - **Tap to click:** Here, a one-finger tap is used to select an item.
  - **Secondary click (right-click):** Clicking or tapping with two fingers is the equivalent of clicking the right mouse button. (Traditionally, an Apple mouse had only one clickable button and no scroll wheel).
  - **Smart zoom:** Double tapping with two fingers will zoom in, then zoom out. This works with web pages and PDF documents.
  - **Scroll:** This is performed by sliding two fingers up or down.
  - **Zoom in or out:** Pinching with two fingers will zoom in; expanding with two fingers will zoom out.
  - **Rotate:** Rotate two fingers to rotate a photo clockwise, or anticlockwise.

- **Swipe pages:** Swipe left or right with two fingers to go back, or to the next page.
- **Open the Notification Center:** Swipe to the left from the touchpad's right edge to open the Notification Center. This is similar to the Charms pane in Windows 8.
- **Three-finger drag:** With three fingers, you can drag items on the screen.
- **Look up/data detectors:** Tap with three fingers to look up a word or a date in the calendar, address book, or from another data source.
- **Open desktop:** Spread your thumb and three fingers apart to show the desktop. This is akin to Aero Peek.
- **Launchpad:** Pinch your thumb and three fingers together to show Launchpad.
- **Mission Control:** Swipe up with four fingers to open Mission Control.
- **App Expose:** Swipe down with four fingers to see all open windows.



Diagrams of the preceding actions are available at <https://support.apple.com/en-gb/HT204895>.

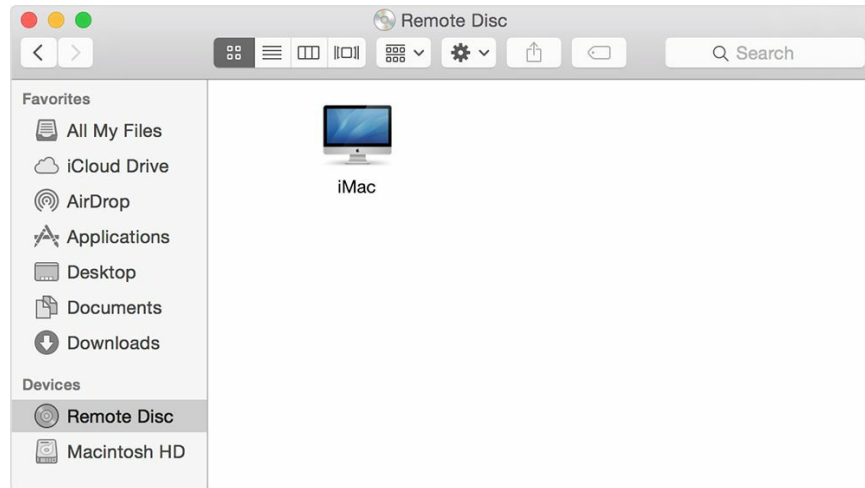
- **Finder:** This is the File Manager GUI, similar to Windows Explorer. The interface is similar to the Safari browser and later versions of the OS support connection to cloud accounts (for example, Dropbox):



- **Remote Disc:** Most systems allow writing to CD- or DVD-ROM media. Normally when you write to such media, you close the disc, writing header and footer data to the media. It is, however, possible (and is common with



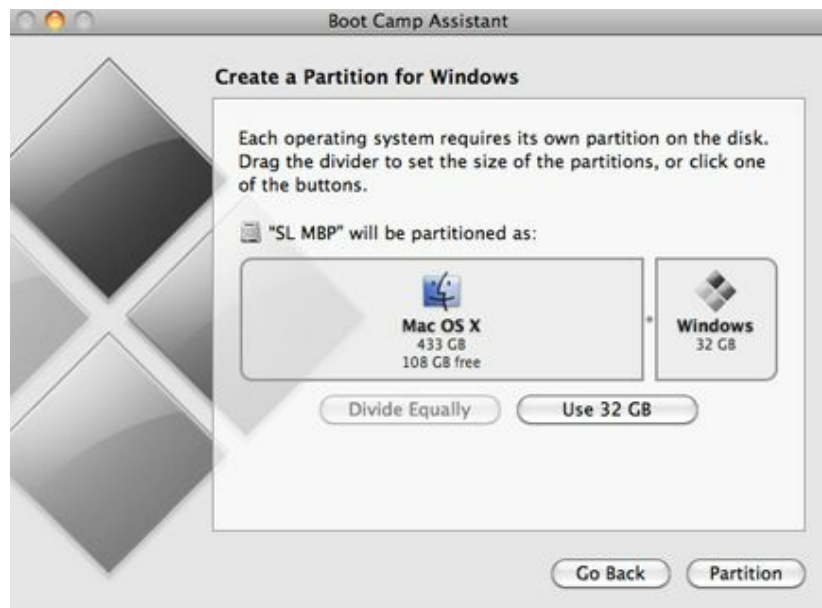
DVD-RW discs) to leave the disc open so that you can use the disc in a way that is similar to an external pen drive, both reading and writing to the disc on different systems. The Remote Disc screen sets up the disc for first use, allowing us to use the DVD-RW as a shareable resource:



- **Dock:** Similar to the Taskbar in Windows, the Dock is the line of icons at the bottom of the screen. Many of the apps on the Dock are themed, allowing you to navigate to the most appropriate section of the OS. Other icons are for regularly used applications, making it easy for you to launch applications.



- **Boot Camp:** This is the multiboot utility, allowing you to make changes to the boot menu. Boot Camp assists in the installation of a secondary operating system onto the PC:





# Basic Linux commands

We are now going to focus on a series of commonly used command-line commands:

- `ls`: Short for **listing**. This is the equivalent of `dir` in DOS. It provides a list of files within the folder, from the current location of the pointer. `ls` command can even color-code files and folders differently, making it easier for you to determine which is which.
- `grep`: A `grep` is a keyword search. It is able to look at the content of files and highlight any files that have the keyword or phrase contained within them. It is short for **global regular expression print**.
- `cd`: Also, `chdir` is used. It stands for **change directory** and is used to move the pointer to a new location.
- `shutdown`: As with DOS, the `shutdown` command can be used to restart or power down the PC. In Linux terms, you can actually specify the run level--that is, the extent to which the operating system will initialize. Run level 0 will power down the system completely, level 1 is single-user mode, and level 6 reboots the system to a full-working GUI.
- `pwd` versus `passwd`: These are very different commands and it is easy to get them confused. `pwd` has nothing to do with passwords. Short for **print working directory**, on its own `pwd` will show you the current location of the pointer, showing the full path name. `passwd` is used to change the user's password for local accounts. The `passwd` will also work with Kerberos and LDAP, and so it can be used to change domain passwords as well.
- `mv`: A UNIX command short for **move**, this is used to move files or directories to a new location.
- `cp`: A UNIX command short for **copy**, this is used to copy files or directories to a new location.
- `rm`: A UNIX command short for **remove**, this is used to delete files or directories, symbolic links (such as shortcuts), and other referenced objects within the filesystem.
- `chmod`: A UNIX command short for **change modify**, this is used to alter security permissions on files or directories, making a file readable, writable, or executable. There are eight different permissions available to a file, ranging from level 7 (read, write, and execute), expressed with the switches `rxw`, to level 0 (none), expressed as ---.
- `chown`: A UNIX command short for **change owner**, this is used to alter the owner of

a file. Ownership can only be changed by a super user (the Linux equivalent of an administrator account), so this command is elevated using the `sudo` command.

- `iwconfig/ifconfig`: Similar to `ipconfig` on Windows systems, you will be able to obtain IP address information for your network cards. `ifconfig` is used with interfaces such as NICs. `iwconfig` is used with wireless cards.
- `ps`: Short for **process status**, this command produces a list of currently running processes. This is similar to `tasklist` in DOS.
- `su/sudo`: Short for **switch user**, `su` changes who is currently logged in without having to log off and log in with the new account. It is used to swap the login for the current session from a standard account to the root account. You can swap to the root simply by typing `su root`.

`sudo` stands for super user do (or **substitute user do**). Usually you need to elevate a command for it to run as it will need more privileges than the currently used account will allow. Elevating a command to run as a super user provides privilege escalation for the command only, not the command window or the active user's environment. While `su` changes the user for the whole session and environment, `sudo` is scoped to only elevate the one command you have run it against. For example, `sudo apt-get KDE` will install the Knome desktop environment, but installations cannot be performed by standard user accounts. This way, my session remains locked at user level, so if I am hacked the environment is still secure.

In the Microsoft world, this is analogous to both the Run As option and, to a degree, also User Account Control.

- `apt-get`: The **advanced package tool** is a clever little chappie! It is a command-line tool that triggers not only the installation of an application, but checks against file repositories online to download the installation files needed to install an application. If there are dependencies not currently installed, the user is informed and these can be downloaded as well. `apt` was originally designed for use with offline installer files (the `.deb` package), but is now widely used across Debian, OpenSolaris, and Apple systems.
- `vi`: Short for **visual**, this is a simple text editor built into the UNIX platform. `vi` is similar to the old Edit tool, which used to feature on earlier Windows systems. Similar to Notepad, it allows you to alter script and initialization files.
- `dd`: This is a command tool used to copy and convert files from one format to another. `dd` is a low-level copy solution and can even back up boot sector information on a hard drive. While the copy takes place, the data can be altered

and converted, for example, from ASCII to EBCDIC test encoding, which was its original intended purpose.

This is a bit of a history lesson, as we tend not to worry too much about encoding, but the **Extended Binary Coded Decimal Interchange Code (EBCDIC)** is an eight-bit binary system used on IBM mainframes. If you downloaded a file, say a BMP picture file from a fileservers using Telnet, but set the wrong coding, you might download it as ASCII data. As it is in the wrong format, `dd` can be used to convert it back into a usable binary file.



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Best Practices for macOS (3:10):** <http://www.professormesser.com/free-a-plus-training/220-902/best-practices-for-mac-os/>
- **Best Practices for Linux (3:13):** <http://www.professormesser.com/free-a-plus-training/220-902/best-practices-for-linux/>
- **macOS Tools (5:03):** <http://www.professormesser.com/free-a-plus-training/220-902/mac-os-tools/>
- **Linux Tools (4:31):** <http://www.professormesser.com/free-a-plus-training/220-902/linux-tools/>
- **macOS Features (6:39):** <http://www.professormesser.com/free-a-plus-training/220-902/mac-os-features/>
- **Basic Linux Commands (13:31):** <http://www.professormesser.com/free-a-plus-training/220-902/basic-linux-commands/>





## 902.2.2 Given a scenario, set up, and use client-side virtualization

In the past, IT developers decided to focus a hardware system on performing one specific job. However, we later learned that the server might be very busy at certain times of the day when demand was high, but idle for most of the rest of the time. Rather than continuing to buy more and more kit for each purpose or service offered on the network, it made sense to put the machine to better use by combining several roles onto the server. That was OK to a point--if the server became very busy because it was a peak time in the day and it was also having to run other services as well, the machine would struggle to handle both jobs at the same time leading to a performance drop, or worse still, the server may crash.

We tried **dual-booting** a machine where it was going to be used for different purposes. My office PC is in fact triple-booted as a Windows 8.1 machine (for general use) and a Server 2012 R2 server working as a domain controller, and also runs our sales CRM system (only used at certain times of the day) and a Windows 7 game server (as I play a lot of very old adventure games that won't run on W8, even in compatibility mode).



# Purpose of virtual machines/hypervisors

What if we could have all three environments available at the same time sharing the hardware resource? Now we can. A hypervisor (Virtual Machine Manager) is an environment that manages the control and flow of data to the hardware. Through the use of a hypervisor, the RAM addresses can be shared among the active operating systems. Each OS is a contained environment. You can even create your own domain within one PC!

- **Type 1:** Hypervisors do not need an operating system present. They communicate directly to the hardware and allow a series of guest OS virtual machines to run in parallel. These are known as **bare metal**, or **native** hypervisors.
- **Type 2:** Hypervisors require the operating system to be loaded first. Here, the host OS's kernel performs some of the roles for the hypervisor, allowing further OSes to be run on the machine as guest virtual machines.

While still a key selling point, and effectively the cloud is just a hypervisor that is available through the internet, the concept of a hypervisor has been around since 1967, where it was used with early SIMMON and CP/CMS mainframes.

Through cloud solutions, such as AWS and Azure, we can spin up a VM from an existing image, such as a Linux vanilla build, ready to use in a matter of seconds.





# Resource requirements

The processor has to support virtualization, and this needs to be enabled within the BIOS. For Intel, this is referred to as **virtualization technology**. For AMD systems, it is called AMD-V.

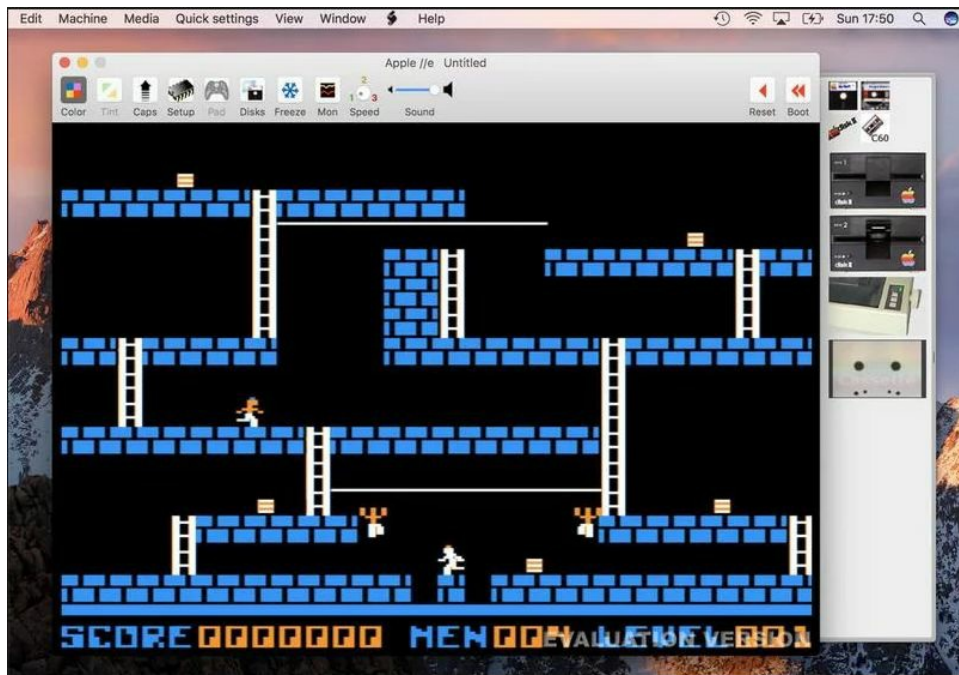
The amount of memory you will need will be greater than the normal amount you tend to use for a host system, but most hypervisors can share memory space between the active VMs. Do not think that if the minimum requirements for a client PC is 2 GB, that if we run three extra VMs then you will need 8 GB; that is not the case.

Each virtual machine stores its filesystem as binary data, known as a VHDX file (or equivalent for other virtualization software, but it is VHD and VHDX on Microsoft systems). You therefore need sufficient space to be able to cater for these files. Usually we create these VHDX files as dynamically expanding, meaning that they grow as more data is written to them, but you should ensure that you have sufficient disk space available on the host system from the outset.



# Emulator requirements

Where virtualization allows us to install several OS systems onto one hardware platform, emulation is the concept of running code through an engine that creates a **shell environment** and runs the application within this protected area. Windows Compatibility is a form of emulator in that code translation takes place allowing the older application to operate using the newer code framework. It is not always reliable, and an emulator may slow down the system.







# Security requirements

Each virtual machine will need its own firewall to be configured, and will also need its own antivirus application. You are increasing the amount of patch management needed with every virtual machine you add onto your network--not only do you need to update the host PC, but also the VMs that it hosts as these machines are security independent from the host.



# Network requirements

Virtualization software also allows us to create our own networks by linking the VMs together, also sharing network resources with the host PC or with the wider network. This is done by creating a virtual switch. The switch is scoped to private, internal, or external:

- **Private:** VMs can communicate with each other only
- **Internal:** VMs can communicate with each other and the host PC via the host network card
- **External:** VMs can communicate with each other, the host PC, and the wider network via the host network card

To communicate, each VM will need an IP address specified in the VM settings to ensure that the NIC is attached to the virtual switch you have created. The IP address needs to be on the same subnet for the VMs to communicate. If you want to communicate with the host, or the wider network, the VMs need to be on the same IP subnet as the host, or receive their IP address via a DHCP server on the network:

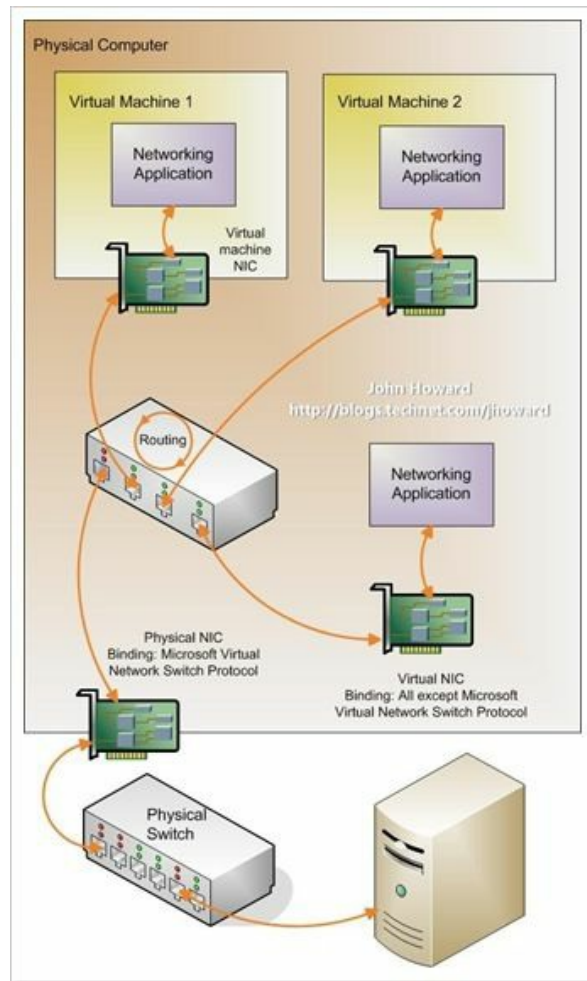


Diagram from <https://blogs.technet.microsoft.com/jhoward/2008/06/17/hyper-v-what-are-the-uses-for-different-types-of-virtual-networks/>.

Virtual machines can also use a shared network address--that is uses the same IP address as the host PC, uses an internal private IP address within the VM itself, and performs network address translation when it needs to cross the logical boundary, just as a router will perform NAT for a private network address.



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Client-Side Virtualization (5:06):** <http://www.professormesser.com/free-a-plus-training/220-902/client-side-virtualization-2/>





## 902.2.3 Identifying basic cloud concepts

The idea of the cloud is to separate our systems and what is housed on them, paying a subscription service for access to our applications. As with on-premises machinery, we can host data and sites, and create apps and databases. The difference is that with a cloud solution we have less cost, and have outsourced our technical maintenance and power consumption--we need not worry about the actual kit, and instead focus on what we are using the kit for. This section will look at the cloud types that are currently used:

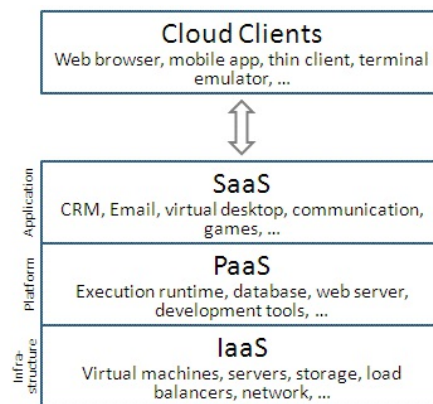


Image source: <http://www.mazikglobal.com/blog/cloud-computing-stack-saas-paas-iaas/>

For the article: <http://www.mazikglobal.com/blog/cloud-computing-stack-saas-paas-iaas/>



# Software as a Service

The cloud solution type known as Software as a Service (**SaaS**) offers a dedicated application for a specific purpose. For example, a virtual desktop may be used for testing purposes. Access to the software is on an on-demand basis. Applications run on the cloud-resident PC and are accessible remotely from any other computer. A common example here is for cloud-based systems to be used for intensive calculations, such as Bitcoin calculations, or the World Community Grid. The customer can remotely access the running PC to use the application on any PC, irrespective of the hardware on the client PC.



# Infrastructure as a Service

With the cloud solution type known as **Infrastructure as a Service (IaaS)**, virtualized cloud PCs and other virtual hardware offer network devices as part of the existing infrastructure, but which happen to exist off-site. These may be load balancers, virtual switches, file servers, or storage devices.



# Platform as a Service

With the cloud solution type known as **Platform as a Service (PaaS)**, virtualized cloud PCs provide specific dedicated services that would otherwise be provided by dedicated servers as part of the existing corporate network. For example, Azure with Team Foundation Server or a Git repository can be used to host software under development and to project manage its creation across the team, including using file versioning. Email servers (exchange online) can provide corporate email from a cloud email server. The **Active Directory (AD)** store can be used to keep a copy of the AD database to be used for authentication and to enforce rules across the network. SQL Server online can offer existing database services as part of a cloud solution, negating the need for expensive, dedicated hardware onsite. A cloud-based IIS or Apache web server can be used to host a corporate intranet or public-facing internet website. This may be an ideal solution for a company that does not want to host their site on-premises.





# Public versus private versus hybrid versus community

In terms of ownership of the cloud structure, we can create a cloud solution with resources shared with the public. Conversely, we can share our resources with our internal staff, or set up an extranet so that staff working away from the office can still access resources. We can even create complex designs where a portion of our network is public-accessible and the rest remains private. We will look at these here:

- With a **public cloud** subscription, costs are low and often some services are offered for free. The main concern here is that there are no guarantees over the security or availability of any data stored on the cloud subscription. This solution is therefore not ideal for a business solution as data will be visible to the subscription provider and security cannot be assured. The solution may be withdrawn at any time, so business-critical data may be lost. An example of this type may be an Azure account where the customer can provision a virtual PC as a server, or as a test Windows 8.1/Linux Ubuntu device.
- A **private cloud** solution is a subscription service offered to a business where legal protection is offered--data is kept private and availability is contractually assured. Private cloud solutions are offered to businesses with guarantees of high availability, scalability, high utilization (such as in the case of thousands of customers viewing a corporate-hosted website), and a lower total cost of ownership than would otherwise be possible, as owning and maintaining a complex server would be expensive.
- A **hybrid cloud** is a combination of some systems that are managed in-house by the company and some parts of the solution that are offered off-site through cloud services. It is usual for a company to host sensitive data internally (such as financial corporate accounts and legal/HR data) while other aspects of the company (such as the public-facing website/e-commerce solution and stock data) can be hosted and managed by the cloud provider.
- A **community cloud** solution is common where organizations decide to share their resources, where there is commonality across the organizations. A solicitors firm, for example, may subscribe to a website where they would be able to look up specific cases or legal compliance information. If a company is planning to meet ISO requirements, they could look up the appropriate information offered by a compliance database. This information would be common to many companies, so

all members would be able to access the same data.

All of the preceding scopes can provide IaaS, PaaS, and SaaS solutions.



# Rapid elasticity

This concept simply means that we can improve, or downgrade, the hardware used to run the virtual machine (or other cloud resource) without having to turn it off first. Most cloud providers can resize your resources automatically so that you are not paying more than you actually need to.



# On-demand

With this concept, we can create cloud resources through a menu system, such as the Azure portal. Resources will be ready within a few moments, as we are not filling out a form and waiting for someone to perform a series of tasks before we can use the resource; the resource is available almost instantly and can be deleted just as quickly. We therefore treat cloud resources as a commodity building and tear it down as needed.



# Resource pooling

A resource such as a virtual machine may need to be highly available. This means that it must be able to withstand a fault. If the host server is not working, that does not matter because other mirror copies of the resource are available on other servers and these may be located at other data centers in other countries as well. This gives us the ability to still access a resource from the resource group, ensuring that our resource is always available.

By sharing the hardware capabilities of the resource pool, we can also allow multiple people to connect to the same resource. In reality, they may connect to a copy of the same resource located on a different server to us. However, the pool will consolidate information--we get the same data.

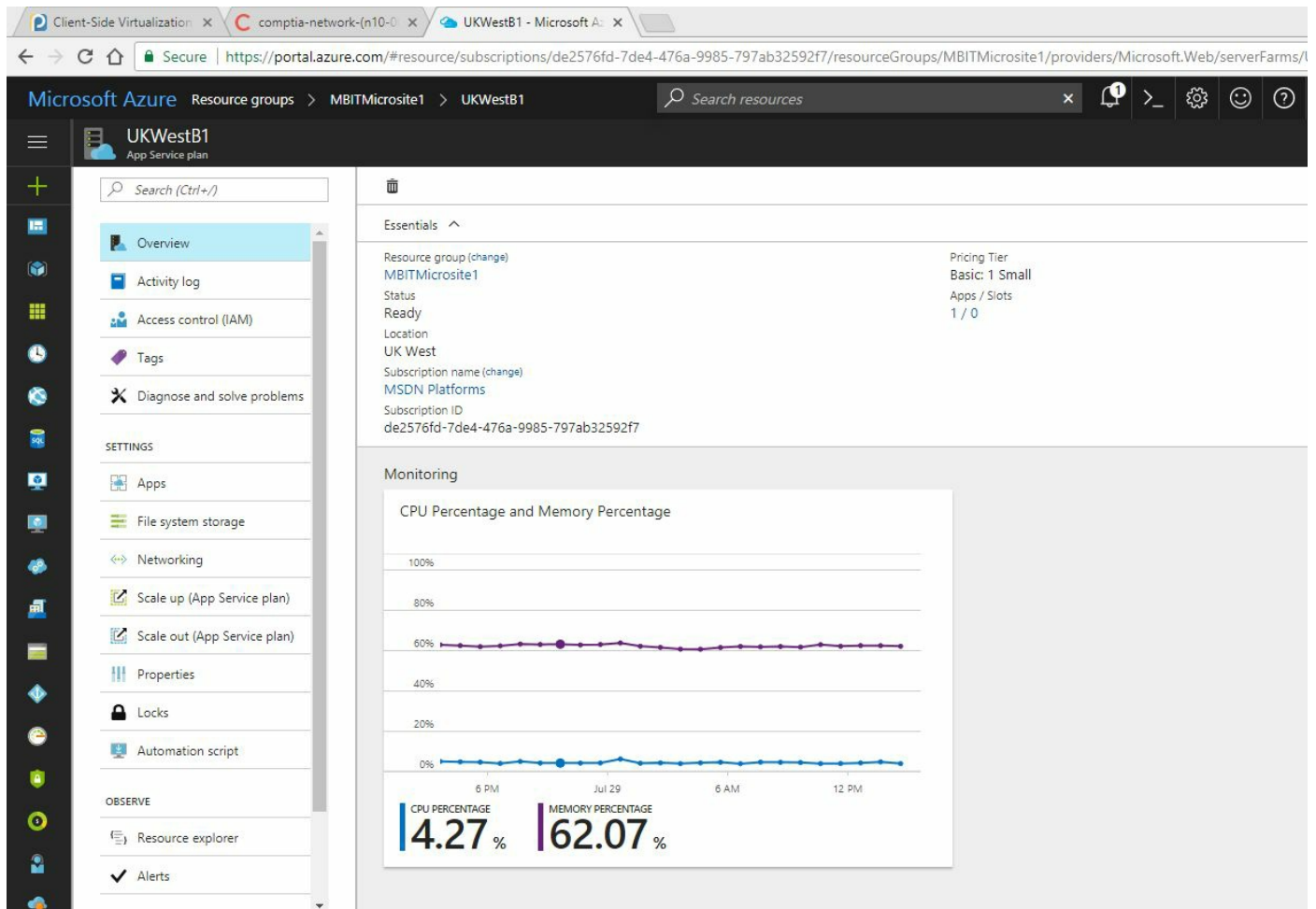




# Measured service

All services offered within a cloud account such as Azure are measured based on the number of processing hours used. Each available hardware profile has a different cost, and the higher the price, the more scalable the resource, as it will support more users, or be quicker. Take, for example, an e-commerce website. If it receives only 100 visitors per day, it is likely that no more than 10 visitors are connecting at the same time, so resource usage is low. We can create a small database, a small file storage area for the site and low processor capacity as these users will not notice any difference.

If I had gone for a more expensive payment plan allowing access to better hardware or connections into the server, or even putting the site into a resource pool, there would still only be 10 visitors connecting at any one time. Should things change, the elasticity of the hardware means the Azure account will automatically realize that more resources are needed, so it will advise you that a change is needed, or you can set this to automatically upscale, should you want it to.







# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide.

- **Basic Cloud Concepts (6:32):** <http://www.professormesser.com/free-a-plus-training/220-902/basic-cloud-concepts/>



## **902.2.4 Summarizing the properties and purpose of services provided by networked Hosts**

In this section, we are going to consider why we use certain network services focusing on how a centralized role may be a better solution, especially on domain networks.





# Server roles

A server is a computer that runs roles that are accessed, and in fact needed, by other users across the network. This section will look at such roles and identify how they are used.



# Web server

Even a client computer can host a website. The Internet Information Services management tool is used to host web files on a PC or server. This allows us to connect to the PC by its IP address, but upon landing on this PC, the PC serves up the hosted web page.

If we involve DNS on our network by placing an A (address) record with the name of `www` pointing to the hosting PC's IP address, then if we navigate in the browser to `http://www.<mydomainname>.com`, the hosting PC will return the index (front page) of the site you are hosting.

In reality, the web files are located in a local folder on the PC--it is very similar to sharing the folder in that a UNC path navigates you to the shared folder, but IIS knows to automatically display the index file if one is present.

Apache is also a very good, lightweight web hosting solution. An Apache server is a dedicated web server with a tiny footprint. Typically, the Apache server will also use MySQL and MyPHPAdmin to manage the server.



# File server

The server can be used to store documents that need to be accessed by several people on different PCs. A file server is a central place to store user documents and other files users may need to access via a shared folder or SharePoint page (which uses the file server as the actual storage resource). File servers use the **Server Message Block (SMB)** protocol to gather the file data from its disks and send it across the network to the client. Apple systems use the Apple Filing protocol, which performs much the same role.



# Print server

The server can render print jobs, manage who can access printers across the network, and act as manager to ensure that documents are printed out in a timely manner. If a manager urgently needs a document to be printed on the same printing device that somebody else is using, and if the manager has priority over the printer, the job will be moved higher in the queue and will be printed faster on the print device. Again, SMB is used to transfer the data to and from the print server, but where we have enabled internet printing, the IPP protocol is also used. For Linux systems, we use the Line Printer daemon.





# DHCP server

A DHCP server will listen for any broadcast packets from non registered PCs. A DHCP server is designed to lease out IP addresses to devices as they need it. Typically, a device keeps the IP address for eight days, after which time the request for another eight days is made.

There are four stages to the DHCP lease:

- **Discover:** A broadcast packet is sent from the new requesting PC across the network. The DHCP hears this packet and the DHCP process starts.
- **Offer:** The DHCP server checks its cache of available IP addresses. If there are sufficient IP addresses available within the range (the scope), then an IP address is offered.
- **Request:** The PC requests to use the IP address it has been offered.
- **Acknowledge:** An acknowledgement packet is sent to the PC which then starts to use the IP address. It is at this point that the lease starts.

An image that may help you to remember the mnemonic is the children's TV series Dora the Explorer.

When the IP address is issued to the PC, other information can also be provided; in fact, DHCP will act as a gateway to other important services and network locations:

- The router default gateway IP address
- Location of the DNS server
- Location of the IIS web server
- Local printer IP addresses for this subnet

It is up to you as a network designer to determine if you want to issue information to your clients through DNS or through DHCP. Usually, it is common to signpost services (for example, IIS and printers) through DNS, but to place the location of the DNS server as a DHCP signpost, without which the new PC will be unable to locate network resources.

When setting up a DHCP scope, it is important to remember that the scope is a logical set of IP addresses, but physically, it is likely that the devices will be local to each other, within the same building, floor, or even room. They exist as part of the same

subnet, and will likely be connected to each other via a switch. They will access the rest of the network outside of their subnet via a router. This poses a problem--by default, routers block broadcast traffic, as is detailed in RFC 1542. Effectively, routers block broadcasts. As the initial stage of the DHCP process involves the DHCP server hearing a broadcast on the subnet, the DHCP server would be unable to service requests on the same subnet if a router was stopping broadcast traffic. It is quite sensible for routers to block broadcasts--without this, a network storm would be created as your new PC attempts to ask the entire internet for the location of a helpful DHCP server.

The DHCP server is significant on the network, so it is the role of the network architect or manager to approve any new scopes added to the network. Your network might have several DHCP servers, or one for every subnet on the network, or possibly one at each branch of your organization. To avoid conflicts, the scopes have to be checked, the scope activated, and the DHCP server authorized before the DHCP starts to issue new IP addresses.



# DNS server

This role is usually dedicated to a server that is capable of serving requests across a portion of the network. The DNS server regularly receives information from devices, acting as a kind of phonebook to the devices, offering lookups or resolutions and helping the PC to find where a network resource is located. DNS is at the topmost level of the directory services model:

- **DNS:** A lookup service that translates name requests to resources or other devices to their IP address
- **DHCP:** The service that issues an IP address to a MAC address
- **Address Resolution Protocol (ARP)/RARP:** A local table or cache, stored on each PC, that describes which IP address is used by known local MAC addresses

DNS is a database of known resources. Referred to as a **zone**. Different domains can each be services within one DNS server.

A request can be one of two types:

- **Forward lookup:** This is a resolution from the name to the IP. This is the most common form of lookup used across a network to find where resources are located.
- **Reverse lookup:** This is not common, and on an internal network there is no need to set up a reverse lookup zone. Reverse lookups are typically used for web servers, where the IP address is known, and where we want to determine which web server (from many in a cluster) a particular website is located on.

Within the zone, there are a number of different record types:

- **SOA:** It may be highly possible that you have many DNS servers located within your network. Which one should a newly joined PC start with? The **Start Of Authority (SOA)** denotes the starting point for any new device--this is the primary DNS server within the network.
- **SRV:** The **Service Record (SRV)** denotes key services within the network. Usually these tend to be DNS servers. Other information stored within the record would be the protocol type and port used to communicate with this service.
- **A:** An IPv4 address of a device on the network. The name and IP address are stored.

- **AAAA:** An IPv6 address of a device on the network. The name and IP address are stored.
- **MX:** The location of the mail exchange server.
- **CNAME:** Canonical name. By setting a CNAME, another alias can be used to refer to a known device on the network. This can make it easier for network administrators to refer to resources and devices by using nontechnical names or nicknames to access a particular server. Where a CNAME is known by the client PC, it will then continue to use the CNAME rather than the actual name for the device it is trying to communicate with.
- **LOC:** A location record is used to specify the geographical location record for a device. This is useful if you have different branches located in different cities and want a way of geographically grouping resources.
- **PTR:** Used on reverse lookups, the PTR, or pointer, refers back to the name. Resolution is the opposite of a forward lookup; this time the IP address is resolved to the device's known name.



# Proxy server

A web proxy server is a network role offered to the client where the proxy acts on behalf of the client to obtain the requested resource. The website is loaded onto the proxy only if the requesting URL complies with corporate acceptable web addresses. The page is first loaded onto the proxy server and then the content is forwarded to the client's PC. By doing this, if the website is popular and contains a large number of static areas, information is cached on the proxy, thereby reducing load time for other users on the network.

A proxy can be enforced as a hidden process, so the end user is not always aware that a proxy is in use. Usually, the web proxy IP address has to be added to the browser configuration, but this process can be implemented by Group Policy, or by the proxy server itself (as is the case with Smoothwall systems).





# Mail server

A mail server, such as **Exchange**, is a central repository for emails. Each user's email account and the emails themselves are stored on this server. The server protects the email with high security, and also Exchange is a management system that defines what emails can be sent, allowing you to content--check emails before they are sent. On modern email systems, such as Exchange, security is highly important, so we encrypt email traffic as it is sent through the network. This connection from the client to the email server is highly encrypted using a certificate.

The client computer, through either a browser or offline software such as Outlook, communicates with the email server using POP3 (for incoming mails) and SMTP (to send management information to other email servers, or to send out the emails themselves). For web-based and internet mail, we use the IMAP4 protocol.



# Authentication server

An authentication server approves access to network resources. An example of this might be a federation proxy server located in the perimeter zone (demilitarized zone) of a network, allowing staff members to connect to the network from outside of the physical building (for example, at home) and then create an encrypted session, but where the actual session runs on the federation server, not on the client machine. The client sees through a remote desktop window during their session and they might think that they are connecting using their own client's resources, but this is not in fact the case.

From a security perspective, an authentication server checks and provides access for users attempting to use network resources. For example, you might connect to your bank's web page and want to log in. The web server and authentication server together manage the login process. The web server draws the form that you see; however, the authentication server deals with the password information you send across, and once you've passed, the security check generates a session token for you to use.

In earlier chapters, the most obvious authentication server we discussed was the domain controller.



# Internet appliance

An internet appliance was a dedicated piece of hardware that would allow an end user to access the internet. It was not strictly a computer, and could do little more than view web pages. This is in contrast to a modern smartphone or PC, which are considerably more versatile, where internet access forms only a small part of what they can do.



# Unified Threat Management

**Unified Threat Management (UTM)** hardware is a dedicated server that will scan documents and attachments in emails, or will request them to be downloaded from the internet, and check them for security threats and viruses before they reach the client.

**Microsoft Forefront--Threat Management Gateway** is one such software application that resides on a dedicated server. All traffic goes through this server, so this server acts as a vanguard.

The idea is to have a primary network gateway defense solution--a single **first stop** for all incoming traffic to be analyzed, thereby reducing the need for configuring other systems with a large number of blocking rules. The UTM device is typically a high-performance server capable of acting as a security gateway, performing antivirus sweeps of data sent through, as well as firewall regulation. Client requests to access sites would be sent to a proxy server and checked that they meet corporate policy before allowing potentially unsavory traffic onto the internal network. By working with the proxy server, the download takes place away from the client machine, and if the download is acceptable to the security policy, the downloaded file is then copied across to the client. To the client, the process does not seem any different from a normal download; however, client requests are being dealt with by proxy.





# IDS/IPS

In an earlier chapter, we looked at host-based intrusion software, such as Sophos or Norton Internet Security. We identified that HIDS was a passive solution, where HIPS (as mentioned) is preventive, stopping the attack as it happens by screening files in use.

These devices are often dedicated hardware resources that accompany the firewall, offering logging and prevention services. The **Intrusion Prevention System (IPS)** uses heuristics (common patterns in data) to determine if the data is a threat to the network (for example, a virus signature). The **Intrusion Detection System (IDS)**, however, does not stop the traffic from entering the network, but does log the traffic as it travels through the device.

When IDS and IPS systems are placed on the network infrastructure, they are designed to bulk-process a lot of data entering the domain. These are referred to as network-based systems (NIPS and NIDS).

Where the IDS or IPS is software based and located on the client PC, these are referred to as host based (HIPS and HIDS). These programs tend to be resource-heavy in that every file in use is scanned for any known signatures that may look like a data string located on the virus database. Norton Internet Security would be an example of an HIPS.

As you can imagine, if the corporate hardware scoping allows for no margin of production beyond the original scope, the PCs will struggle to run IDS software. This is why it is common to see problems with domestic end-user computers as they did not allocate for the additional demand on the system an IDS system will bring.



# Legacy/embedded systems

The term legacy systems refers to an old, outdated, or unsupported system. It is highly likely that the system will have proprietary, bespoke software built for a specific purpose and will be unable to communicate with a centralized system; therefore, control of the system requires an intermediary step, either bridging software or the direct control of a member of staff where centralized requirements can be interpreted and production output adjusted accordingly. Legacy systems tend not to be updated and are often expensive to maintain if serviced under a long-standing agreement. If the original servicing company is no longer on the market, highly specialized programmers are needed to understand how to communicate with the system.

Conversely, some legacy systems have a small total cost of ownership. For example, if the company is an industrial manufacturer who can see no means of updating a process within the factory, and the original (now legacy) system is still productive, but the code was written decades ago, it may serve to simply hire a programmer as part of the company and provide a decent salary for the person to service the system. An example here would be of a LISP, or COBOL system running a program that will perform a series of actions. There is no need to change the initial requirements, and the machine has no need to communicate on the network at all.

In earlier chapters, I described the ransomware attack that affected NHS trusts across the UK earlier in 2017. It has transpired that some of these trusts were using Windows XP, which has been unsupported by Microsoft since 2014, but some trusts made an arrangement with Microsoft for bespoke support for 2015, but even they have been unprotected for two years.



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide.

- **Network Services (9:26):** <http://www.professormesser.com/free-a-plus-training/220-902/network-services/>



## **902.2.5 Identifying basic features of mobile operating systems**

In this section, we are going to look at some of the features specific to particular operating systems you will encounter on mobile devices.





# Android versus iOS versus Windows

Starting with Apple iOS, this is the OS you will encounter on the iPhone and iPad. It uses UNIX, but is a closed source software, meaning that the core source code is not available to the public. Apple iOS is only available on Apple products--you have to go into an Apple store and purchase the hardware. The software is bundled onto the device as with a mobile phone. Any application released on the Apple store has been tested and approved to work on the device, so there is less of a chance of an application not working, which is a common problem with Windows systems as the hardware components vary on PC builds, which causes instability.

Google Android is maintained by the Open Handset Alliance. Its code is therefore checked by a community of programmers, ensuring that it undergoes rigorous testing before it is released as a new version. It is based on the Linux operating system and is designed to be hardware-agnostic. It is open source, meaning that the source code is available. Apps for the Android system are available from Google Play or from the Amazon App Store.

Windows Mobile is a variant of Microsoft Windows designed to work on the Windows phone. It is closed source. The OS is based on Windows NT. Apps are available through the Windows store and, as with Apple, the apps are tested before being allowed onto the store.

To ensure that the screen is displaying the right geometry (for example, portrait or landscape), the phone has a built-in gyroscope to determine which way around it is being held. Also present is an accelerometer capable of measuring the speed of the phone's movement, so your phone can record your steps and act as a pedometer should you want it to do so.

In order to work correctly and realize where the user has pressed on the screen, the device needs to be calibrated. The calibration tool asks the user to press the extreme corners of the screen, but the **screen pixel density** can skew where it thinks you have pressed.

By using the Global Positioning System, we can triangulate where the phone is to within two meters on the planet. The GPS sends a radio signal to four neighboring satellites. The relative distances translate as x/y coordinates. Through this we can record this data against time--a process known as **geotracking**.

Perhaps you don't have a phone signal, but are connected through Wi-Fi to your home router. In that case, Wi-Fi calling will help you as you will be able to use this feature to channel the phone data through your Wi-Fi instead of the telecoms provider. Some companies, such as EE, allow this, but it is an extra service and has to be enabled. Some Android and Windows phones bought through other providers do not allow Wi-Fi calling, but it is common on iPhone, Blackberry, Android, and Windows phones when bought through the provider (for example, EE).

Each phone GUI has its own distinctive look and feel--Windows has its tiles menu system, Apple has the Dock, Android has the swipe-able screens and pull down buttons. The **user experience (UX)** design is what gives the phone its distinctive character.

- **Virtual assistant:** Alexa, Cortana, and Siri are three people you will grow to love, or to hate. They give you the ability to speak to your phone and ask it to perform a change to your physical environment, such as to turn on a light (if linked to your home automation network), as with the Amazon Echo. These virtual assistants will listen out for an instruction from you, triggered by you directly addressing it (for example, Hey Cortana, tell me a joke). The VA is internet-connected, so can perform research and open up web pages for you, or even play a music track from your music library.
- Mobile software development kits are a suite of command codes and tools you can use to make your own mobile app. They typically also contain an app creator/editor, allowing you to plan, format, and code your app. An APK is an Android application package. This is the file format used to install an app onto your Android operating system.
- In Windows, the process of installing an app from a local application package file is called sideloading.
- An emergency notification system is a method of broadcasting a message to alert a large group of people of an emergency. They are a way to alert the public of a problem, such as a tsunami, an air-raid, or other emergency situation. Some local governments are now using ENS software to notify groups of people in the event of an emergency. In the UK, this is a replacement for the United Kingdom Warning and Monitoring Organisation and the Royal Observer Corps' emergency signal, which was designed for civil defense and used throughout the 1960s and 1970s, but was put out of service in the 1990s.
- Mobile payment services are available on most mobile phone providers. They use Near Field Communication so that you can pay for an item at a till in much the same way as you can with a debit card, using contactless payment. PayPal, Amazon Payments, and Google Wallet all have mobile options. First, you have to register

your phone number with the provider, who sends an SMS message with a PIN code. We then enter the PIN, authenticating the phone number as valid. The user then enters their debit card number into their profile on their mobile wallet, on the phone app.



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide.

- **Mobile Operating System Features (6:32):** <http://www.professormesser.com/free-a-plus-training/220-902/mobile-operating-system-features/>



## **902.2.6 Installing and configuring basic mobile device network connectivity and email**

Considering how mobile devices can be used to connect to the network, we are going to focus on the different signals and carriers available and discuss how each functions.





# Wireless/cellular data network - enable/disable

A hotspot is an area where the user can connect to a wireless access point (the area where the device may connect and the user authenticates to the network is considered hot). Once connected to the Wi-Fi router, the device can act as an access point for other mobile devices within the local area.

Working regularly across the UK, I visit a number of hotels. My laptop is not always able to connect directly to the Wi-Fi router, but my phone often will. As that is the case, I then use my phone as a hotspot and tether my laptop directly to it by using a USB cable. This extends the internet capabilities of my phone to the laptop as well.

Airplane mode, also known as flight mode, or offline mode, prevents the mobile phone from being able to send and receive calls but also blocks Bluetooth and Wi-Fi radio transmissions. The problem is not so much the Wi-Fi signal, but the fact that the cabin crew get crosstalk and interference caused by your phone call through their headphones, which to them is an irritant. By enabling airplane mode, the other transmission types switch off. You can override this for Wi-Fi and Bluetooth, turning them back on.



# Bluetooth

As a connection system, Bluetooth is a reliable, easy-to-use, ubiquitous facility now present in most modern smartphones and laptops. Bluetooth enables point-to-point connections with an other device, such as a Bluetooth keyboard connecting to a smartphone, and works by sending radio signals to the connected device. Bluetooth operates on the 2.4 GHz band and typically would send 1 Mb/s over 10 meters, although recent versions of Bluetooth are being developed that increase the speed and range at reduced power. Bluetooth is the connection system of choice for local gadgets or personal accessories (for example, a Bluetooth headset, earpiece, or hands-free kit).

Once Bluetooth is enabled, you simply press the Discover button on the device you want to pair with. This has to be within range. If you are connecting to another complex device, such as a phone, you may, for security reasons, set a PIN code, which is generated on your phone and needs to be entered on the device you are connecting to. Once established, a secure radio channel is present between the two devices.



# Corporate and ISP email configuration

As we discussed earlier in the section, email servers use the now rather old **Post Office Protocol (POP3)** to receive emails. The email is stored as a file on the email server and can be accessed by the client either by reading it on the server itself using a web page and its separate **Internet Mail Authentication Protocol (IMAP)**, that means that the email actually stays on the server. However, the client might be using a client email program such as Microsoft Office Outlook which actually downloads the email from the server and stores a copy of it on the client PC as well. To send emails between servers, and also to send emails out of the network to the recipient, we use the **Simple Mail Transfer Protocol (SMTP)**. More secure and more complex than POP3, SMTP also allows us to send security and configuration information between email servers.

- POP3 uses firewall port 110
- SMTP uses port 25
- IMAP uses port 143

In addition to this, we use the Secure Socket Layer protocol to encrypt a channel between the two endpoints (email server and email client) so that the email cannot be intercepted en-route. The email is sent as web traffic using port 443 and is protected by a certificate installed on both endpoints.

**Secure/Multipurpose Internet Email Extensions** allow you to attach a digital signature to the email for the purposes of non-repudiation. In other words, the digital signature contains information about your user account, as well as a timestamp proving that you are the sender. S/MIME is also responsible for ensuring that the certificate to be used by the client actually reaches them and installs before we can send an encrypted email.

The most common email server used is Microsoft Exchange, which is a suite of tools controlling email user accounts, email security, as well as the mailboxes themselves. It integrates tightly with AD, so changes made to user account objects in AD are also updated in Exchange.



# Integrated commercial provider email configuration

As well as using these providers for personal, often free accounts, Google Mail, Yahoo, Microsoft's Outlook.com, and Apple iCloud all feature as business-capable versions. These business accounts allow you to not have to invest in Exchange, which can be complex to set up, but instead to integrate your domain with a third-party provider. Google Mail, Yahoo, and Outlook support both POP3 and IMAP email protocols, but Apple only supports IMAP.

One key feature of using a third-party provider other than Exchange is that there is no need to expose part of your network, or to set up a hosting server in the perimeter network (exchange proxy); rather, your staff can use a web link to get to their emails irrespective of where they actually are. Naturally, they can use a mobile phone web browser and navigate to the page to then view their emails.





# PRI updates/PRL updates/baseband updates

Our mobile phones are radio transmitters and receivers. The baseband radio processor connects us to the cellular wireless network. It has its own firmware and operating system separate to the Android OS you might see on your iPhone. The baseband OS is updated regularly and these updates are sent periodically to the device across the telecoms network. This happens invisibly--there is no administrator setting for us to configure here.

The preferred roaming list is another seamless invisible update. This is used for **Code Division Multiple Access (CDMA)** networks, and this is the 3 G/4 G high-bandwidth mobile networks you will commonly see across most towns. The roaming list is like a routing table in that it explains how to roam using your service provider. If you swap service providers, the roaming partners will feature on this PRL list.

Product release instructions are also invisibly updated regularly. These are radio settings, ID numbers, country codes, and other key information that explains to the phone how to communicate with your mobile provider and use their network.

Your phone has a unique number, just as a chassis VIN code is stamped onto a car as it leaves the factory. The International Mobile Station equipment ID is used by your mobile phone provider to allow or to bar the phone on the network.

The International Mobile Subscriber Identity identifies you as the user of the phone. The IMSI is located typically on a SIM card and it is why the SIM card is associated to your mobile provider's account. If you need to upgrade your phone, you replace the SIM card and add it to the new phone; in this way your phone account will be associated to the new phone.

Just as a laptop can create a virtual tunnel through which we can send an encrypted session, your mobile will also access some resources using a VPN tunnel. Your phone will likely support multifactor authentication, so session tokens can be used to connect to a VPN. These may contain a username, password, details from a fingerprint scan, or other information that forms the key used.





# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide.

- **Mobile Device Connectivity (5:51):** <http://www.professormesser.com/free-a-plus-training/220-902/mobile-device-connectivity/>
- **Configuring Email on Mobile Devices (4:24):** <http://www.professormesser.com/free-a-plus-training/220-902/configuring-email-on-mobile-devices-2/>



## 902.2.7 Summarizing methods and data related to mobile device synchronization

In this section, we are going to consider some of the data that is actually synchronized between your phone and a central server either within your domain or a service that you have connected to. The types of data that can be synchronize include:

- Contacts
- Programs
- Emails
- Pictures
- Music
- Videos
- Calendars
- Bookmarks
- Documents
- Location data
- Social media data
- eBooks



# Synchronization methods

Synchronization can be triggered either by the server (when sending to all clients, this is known as a **push**), or by the client (when receiving from the server, this is known as a **pull**).

When we synchronize to the cloud, any changes are copied across to the cloud account. When we synchronize to the desktop, new files from the cloud account are copied onto the local device. Naturally you need to know that you have sufficient disk space available if you are populating an entire music library onto a new phone!

Before we can connect to the provider, we have to create a secure session. As part of this, a handshake process takes place in which the device sends a challenge to the server and the server also sends a challenge to the client device. Both have to pass, at which point both trust each other. This is referred to as mutual authentication.

Once you have passed the authentication test, a session token is generated that is used by your device to confirm that it is still you. This is a pseudorandom ID string that is effectively an ID badge while the session is live. Every time you attempt to access a new service, the token is used to identify you, but the advantage is that the user is not prompted to put their password in every time they want to navigate to a new area or download a new file.

The cloud account can also be shared with a PC, but this requires the installation of a client for desktop software, which serves much the same purpose--it allows the device to use mutual authentication and a single sign-on into the client's account (for example, iCloud).

If you are planning to connect your mobile device to your PC with a view to transfer files across, this is possible, but may require specialist cables to do so, which are proprietary to the manufacturer. Apple's cable is proprietary, connecting its devices to a USB port. Newer iOS devices use an 8-pin Apple lightning to a USB connector, whereas the older iOS devices used the 30-pin to a USB connector. Android and Windows Phone both use USB-B (or MicroUSB) to USB-A cables.

Of course, it may be easier to send the data via your wireless router by sharing the folder on the device.







# Exam questions

1. What is the tool used on Apple systems to automatically back up user data?
  - Answer:
2. The Finder search facility will check which three areas for content?
  - Answer:
3. What subscription system is used to centralize user files, settings, and also passwords?
  - Answer:
4. I want to check the IP settings of my wireless NIC using a Terminal window. What command do I use?
  - Answer:
5. I need to run a command to install an application from the Terminal window, but am logged in as a standard user. I need to elevate privileges for the action only and not elevate my user session as that would be a security risk. What command do I use?
  - Answer:
6. I need to edit a text file in the Terminal window. Is there a tool I can use to do this?
  - Answer:
7. What is the difference between a public cloud and a private cloud?
  - Answer:
8. What is the purpose of a federation proxy server?
  - Answer:
9. What is the difference between an IPS and an IDS device?
  - Answer:
10. What is meant by the term "Rapid Elasticity"?
  - Answer:



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Mobile Device Synchronization (3:34):** <http://www.professormesser.com/free-a-plus-training/220-902/mobile-device-synchronization-2/>



# Summary

This chapter focused on the equivalent tools on Apple and Linux systems. We also looked at how we can virtualize our systems to make the best use of the resources, as well as how to have multiple VMs, each with a different operating system running on the same physical hardware. We took the analogy further by considering how to create our virtual machines, not only on hardware we own, but on subscribed accounts--the cloud. We looked at the different theories on how we can create our own VMs in the cloud and how to extend this to create an entire network that exists solely in the cloud, where it exists as a highly available resource. We also looked at how to create an application that is hosted in the cloud without the need to create a resident virtual machine to run it on.

Coming back to Earth, we considered different servers and their roles from a productivity context, plus security applications we can use to protect our machines, and separate our networks from outside attack.

We then considered the operating systems you would find on mobile devices and looked at some of the features unique to them, and then considered how to network using mobile devices, especially regarding the sending of emails. Finally, we considered how to synchronize our data across devices.





# Security (902.3)

The major reason for securing the network is to protect from an attack. An attack is defined as any action deemed improper on the network which will affect productivity, or by its action, expose data to theft, damage, or removal from the network. We will categorize each of the different attacks you might expect to encounter on an enterprise network, looking at their severity and how they affect the network.



## **902.3.1 Identify common security threats and vulnerabilities**

Within this section we are going to identify different software-based security threats and categorise them:



# Malware

Mal is French for **bad** but in cyber terms it is a catch-all term to mean any unwanted activity. Historically, a virus was seen as a separate and more damaging category whereas malware simply referred to advertising pop-ups or software that would get in the way of productivity, but in itself is not inherently bad or damaging to data stored on the network.

CompTIA does not make this distinction and uses malware as a catch-all term to refer to any malicious activity on the network not deliberately enacted by an end user.

- **Spyware:** Some software install as a background service and capture key presses (a key logger), or take screenshots of your actions in the hope that these may contain vital information such as passwords, or account details. Data is copied secretly from the hard drive to an external source, such as to a web server. In short, Spyware is anything which will spy on you.
- **Viruses:** A virus is more dangerous. This is a piece of code that deliberately alters the working of the system with a view to stop normal processes and damage your productivity. A virus is a catch-all term for a variety of several thousand pieces of adaptation code that have been injected into legitimate files. When the file is run, the extra code injected into the file is also run, which performs unexpected activities aimed at destabilizing the system. A virus has therefore a damaging effect on the system and also has the ability to copy itself to other files, and even traverse the network affecting files on other systems across the network.
- **Worms:** Whereas the term virus is a general term for any malicious code that is damaging to the system, those which specifically do replicate and spread to other computers are referred to as worms because they bury (hide) within the system and tunnel through your security and propagate across the network. A worm, in contrast to a virus, is a standalone piece of software that is capable of propagating automatically, without any interaction with the user. Viruses spread the original infected file across the network, so the same damaging action, such as a pop-up message appearing, which must then be clicked by the user, would happen on every infected PC.

The **Conficker Worm** was first detected in 2008. It was designed to attack Windows systems and uses a dictionary attack on user passwords and creates a **botnet** (a series of infected computers acting as a separate network to perform a series of defined tasks). It infected millions of systems worldwide in over 190

countries and is the largest known computer infection.

Rumor has it that the Conficker Worm was deliberately created as a cyber warfare attack aimed at destabilizing uranium enrichment plants in the Middle East. These systems were, however, SCADA systems (independent and often using proprietary system software, not generic software such as Windows). The problem was how to get the virus into the SCADA network, as there is an **air gap** (the network is not connected to the internet). In the end, the air gap was breached by a contractor who connected their laptop, unknowingly infected, to the SCADA network.

- **Trojans:** Based on the Greek mythology of the siege of Troy, a Trojan is a file masquerading as a legitimate file, such as a Microsoft Office document, or spreadsheet, but in fact contains an attached virus. There is a deliberate attempt here to trick the user into wanting to open the file as they are convinced that it is a genuine document. Once opened, the file has access and the virus is released.
- **Rootkits:** On Linux systems, the concept of the root area is where all of the critical system files and settings are stored. The Administrator account, known as the root account, is the only account that can make important system changes. Standard users cannot access the core system files. This is different to the Windows system, where the whole file system is exposed. The rootkit is a piece of code that bypasses this security and obtains access to the core root area. On a Windows system, a rootkit affects the bootstrap files and the initial loading, and also the registry.

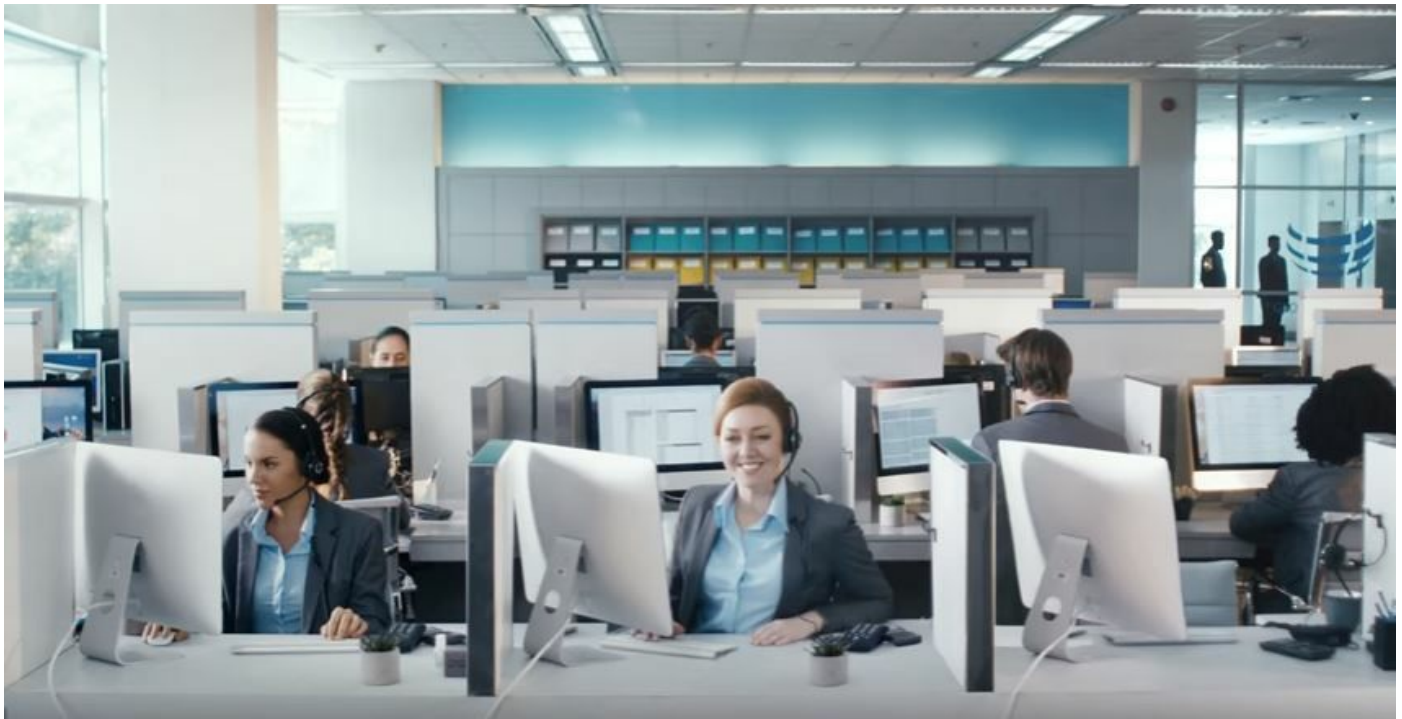


Can a rootkit damage the BIOS? This is an interesting question, as for many years the answer has been no because the software installed on the BIOS is read only--only the configuration changes made can be saved to the BIOS chip. Later rootkits could affect these--one such case was to download a binary image of a newer version of the BIOS that has not come from the original manufacturer or is digitally signed, but instead is infected with the virus code.

- **Ransomware:** A piece of code that encrypts all files on the hard drive and requires that you pay to obtain a key to unlock and decrypt these files is referred to as ransomware because the company is literally being held to ransom. Any payment is made online, usually to a Bitcoin account. There is no guarantee that you will receive the decryption information, but the point is that when the system is encrypted by an encryption key, you cannot control or stop it.

- **Phishing:** The process of a conversation, usually over the phone, in which someone gains your trust and asks you low-level questions about your work which will give them information about the structure of your company, network, data, and other information that will help the attacker learn a picture of the network and its vulnerabilities. The attack may be in the form of an email that looks legitimate, but in fact the hyperlinks will send any data back to a webserver that is not the company it claims to be. A caller may claim to be from a legitimate company and may ask you to do certain things to your computer, or ask you personal information which may be quite sensitive and by knowing this may allow them to pretend to be you.

"(Phone agent in an office cubicle making a call to a customer) Thank you for taking my call. Before we continue, could you say the first and third digits of your security PIN?...oh..er.. I didn't catch that. Sorry - that's the second and fourth please. Ok - lovely. All gone through.(Turns to the camera. Smiles.) Did you see what I did there? (Smile fades. Serious look to camera. Takes off headset as camera pans away). Narrator: It's a scam. Never reveal your full security PIN even if you think it's your bank calling. Learn how to protect yourself from fraud" Barclays UK Digital Safety TV Advertisement 2017 (<https://www.youtube.com/watch?v=vPJ6irUDmHI>)



- **Spear phishing:** Similar to phishing, the difference is that this is a targeted attack aimed at a specific individual. It is possible that some personal information is known, or the attacker has learned a hobby or some other personal information so

that when the attacker engages in conversation with the target they are able to break the ice or gain trust of the target before then asking low-level questions that may reveal information about the wider organization and how it is constructed.



Be careful when working with contractors here. Initially, they may not be fully security cleared and may be quite convivial and good to work with, but you do not know where their allegiances lie. Next week they may be working for your competitor and will have some inside information about the structure of your company. For this reason, some companies prefer to use either contractors who have completed security clearance prior to being admitted on to your site, or avoid the problem by outsourcing the work to a company, or person who can work off-site.

The attacker might not be an external person but actually a member of your own organization. A **watering hole** attack, not covered in the course, but is a subset of the speak phishing attack type where a member of staff may have a conversation with you in the canteen, or during a coffee break. The idea of the watering hole is just that--an area where people may meet to stop work and chat, such as stopping for a cup of water at a water fountain (the watering hole). Here, they might discuss company plans, strategic plans, staff holiday times, and so on.

- **Spoofing:** Not necessarily malicious but the act of pretending to be someone else with a view to play a trick on a member of staff, or pretending to be someone known to the member of staff with a view to elicit information from them is known as spoofing. There is some crossover here with speak phishing in that the attacker is pretending to be someone the target would be aware of and because of this may relax their guard, or convey more specific information than they otherwise would do.
- **Social engineering:** In its bluntest form, if someone were to ask you What's your password? this is effectively social engineering. The act of engaging in a conversation in its most broadest form in order to elicit information from an individual is referred to as social engineering because you are manipulating the conversation to your own ends.
- **Shoulder surfing:** The act of looking over the target's shoulder to see what is on their screen, or to read information on a paper document they are holding is known as 'shoulder surfing'. This would also count journalists who have taken a photograph with a long lens of ministers who have held documents in their hand and from this their meeting notes can be obtained. For convenience, end users sometimes keep important phone numbers or passwords on post-it notes dotted



around their screen. This should be avoided and as a security specialist you should discourage this for the reason that other people will also obtain this information and attempt to be them.

- **Zero-day attack:** Once you have installed the operating system from an installation disk, the system may well work but the software files used are now several years old. A lot has happened in that time and a series of updates and patches have been produced by the manufacturer to fix vulnerabilities that have been discovered since the original release of the OS. These patches need to be installed (part of the concept called **system hardening**) before the user can use the PC. Any attack that uses one of these vulnerabilities that have subsequently been patched are referred to as zero-day attacks, because at the time of the install the vulnerability is still there and the system has not yet been patched. Until it is, the system is vulnerable by these suites of attacks.
- **Zombie/botnet:** Some attacks ask other computers to run background services without the knowledge of their end user. Worms cause this additional code to be spread to other PCs and then to trigger the code. When a computer is performing a malicious attack without the knowledge of the end user that this is taking place. This PC is referred to as a zombie as it cannot control its own actions, rather the malicious code is running irrespective of the OS. Where a collection of zombies work together to perform an attack (for example, a **Distributed Denial Of Service (DDOS)** attack against one specific hardware component on the network with a view to stopping the component from functioning). The problem with a botnet is that the virus spreads just as fast as the technician, or anti-virus software can repair the damage. As a technician, your priority should be to contain the infection whilst keeping essential services running.

Back in April 2017, the UK National Health Service was hit by a major nationwide attack affecting most NHS trusts. Some trusts decided to close their IT networks entirely until the problem could be resolved. This involved investigation from the National Cyber Security Centre, police, and other authorities whilst the IT technical teams within the trusts repaired damaged systems by reimaging, or completely rebuilding the PCs. The reason for the ease of the attack was that the NHS still used Windows XP on most of its systems for two reasons:



- They did not want to pay extra costs to upgrade several thousand PCs
- A lot of old software is still in use as part of their production network, which could not be upgraded to be used on later systems that were still supported by Microsoft

This was a gamble which did not pay off. Now, NHS Trusts are re-evaluating their strategic response to attacks and are looking to upgrade to Windows 10 Client. I personally recently taught a Windows 10 course to an NHS Trust at Welwyn-Garden City in July.

- **Brute forcing:** This type of attack is designed to continually attack a specific portion of the security on a network. One possible brute-force attack would be to attempt to use random characters to guess a password, but the password guess is attempted thousands of times using different characters each time. This is often used at the end of IT action films such as the Dan Brown movies, or **WarGames** (<http://www.imdb.com/title/tt0086567/>), where you see a computer use different characters to guess a missile launch code.



"A strange game. The only winning move is not to play....

... How about a nice game of chess?"

WOPR: Wargames (1983))

In reality it is not usually so dynamic. A brute-force attack is a guessing attempt and can be targeted against a specific part of the network; for example, to access a website hosted on a web server as here security is often more relaxed than Kerberos authentication as most websites do not use Kerberos unless they are internal sites (intranet).

Another type of brute-force attack might be a firewall port scan--here, we have 65535 TCP and 65535 UDP ports. Most of these are closed but which ones might I be able to use to send data into the network? By trying each port in turn and seeing if we get a response, we are performing a 'brute-force' attack. This can be done simply with software such as ZenMap (NMap) or Nessus, which perform a port scan and are legitimately used by network management to check which ports are actually open.

- **Dictionary attacks:** As part of this section is the concept of a rainbow attack. A rainbow table is a list of common words used in passwords (such as Password) but also other permutations of this word (for example, Pa\$\$w0rd). Software used to perform such an attack (and can be legitimately used to test the security of a network by network managers) is Cain and Abel, available at <http://oxid.it>. This program is used in the Professor Messer videos you will find that accompany this book.
- **Non-compliant systems:** If you have a system health validator in place on your network, all PCs need to meet a certain compliance level you have defined. For example, you may decide that all PCs need to have been updated with the latest approved updates and a virus scan must have been completed and reported as clean using the latest virus dictionary. If they do not meet these standards, they are said to be non-compliant and therefore should not be able to access network resources until the system is again compliant. Enterprise networks use DHCP to provide a separate IP address in a different scope where remediation can take place. When the PC is finally compliant it will receive a valid IP address on the main network.
- **Violations of security best practices:** As part of the **Defense in Depth** model, there are non-technical safeguards, such as end-user training. Where an individual chooses to, or due to a lack of information or training (or compassion!), decide to ignore the security put in place, a violation is said to have occurred.

Here is an example of a security violation:

"While entering the building through the rear security door, an employee realizes that he has left his car keys in his car door. He has already swiped his badge to open the door, so he props open the door with his briefcase while he returns to the car to retrieve the keys. The door is in view at all time and no one else enters the door while it is propped open. He locks the car door behind him and also the security door once he is in the building. "

Although no security attack took place during this time the man was in breach of

security regulations.

- **Tailgating:** The act of following another person who has security clearance through a security door, or checkpoint and by so doing not having to stop to be checked or to use your own ID is referred to as **tailgating**. Sometimes someone wanting to breach the physical security may dress up as a delivery driver, or a pizza-delivery person with a view to be let through a security door by an unsuspecting person because your hands are full.
- **Man-in-the-middle:** Nothing to do with Michael Jackson songs, I assure you! A man-in-the-middle attack can only take place on the local subnet. It exploits the fact that the Address Resolution Table (ARP) is not encrypted. This table is a record of all learned MAC addresses and the IP addresses associated to it. A man-in-the-middle attack is where the attacker sends an ARP request to both the server and the end user's PC. Both report their MAC addresses. The attacker's PC sends an ARP packet advising both other PCs that the MAC address has changed. As a result, all traffic goes through the attacker's middle PC where packets can be read and information recorded.



The Professor Messer video in the Security+ series covering man-in-the-middle attacks has a demonstration on how to attack a wireless router and obtain its login password using a man-in-the-middle attack. The software used is Cain & Abel. The video is available at: <http://www.professormesser.com/security-plus/sy0-401/man-in-the-middle-attacks-2/>

This attack can be difficult to protect from as the ARP table is not encrypted. Using Wi-Fi encryption will help to some extent as will the use of a digital signature so that packets sent to the server can be checked for authenticity.



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand ,and provides an excellent overview and accompaniment to this study guide.

- **Common Security Threats (18:18):** <http://www.professormesser.com/free-a-plus-training/220-902/common-security-threats-3/>



## **902.3.2 Compare and contrast common prevention methods**

The Defense in Depth model covers physical as well as technical security. This section will focus on actual physical restrictions, both active and passive, which can be used to stop or slow down access to resources within the site.





# Physical security

So far we have looked at Defense in Depth from a software perspective, but what about actual physical access to resources? This section will look at the physical passive and active systems we can use in combination to deter, or to stop would-be attackers, thieves or other ner-do-wells from compromising your systems by gaining entry inside of your building.



# Lock doors

If a door is locked, then it needs to be unlocked to enter, or an alternative entry method found. Door locks can be overcome by copying or stealing a known good key. Locked doors within offices usually also use key fobs.



# Mantrap

It is not as painful as it sounds, a 'mantrap' is an area such as a corridor with two different security doors, typically with two different PIN codes needed to clear the mantrap area. A traditional mantrap is a 'buffer zone' between two security doors often with a one-way mirror window so that a security guard can view who is traversing the corridor and if necessary lock the unauthorized person between both doors until a guard can investigate the problem.

Mantraps are common in airports and prisons where movement has to be restricted. They can be found between different security zones.





# Cable locks

To protect from hardware theft devices, such as the PC chassis, monitors or laptops have a special cable lock port. This is a rectangular hole in the outer plastic allowing access to the metal frame within. A barrel lock (also referred to as a **Kensington lock**) connected to a steel mesh, braided cable is used. The **Barrel** key attaches to the metal frame of the chassis within the device and the cable is looped around a table leg and corner making it extremely difficult to remove the device from the desk. Only the technician (and possibly also the end user) would know the combination to unlock the device and through training the end user is encouraged to always make sure that the device is locked when present.



**Securing physical documents/passwords/shredding:** It is common to file important paper documents within a lockable filing cabinet. A paper document has a shelf life after which point it does not need to be kept. At this time, the paper document would be shredded, by feeding it into a cutter which will cut the paper into thin vertical strips. As it is possible to re-piece these back together, it is more secure to buy a cross shredder which cuts the document into tinier diamond pieces.





# Biometrics

The process of using a part of the body which has a unique identifier such as a voice print, retinal scan, or more realistically, a fingerprint is the concept of biometrics.

Additional readers such as a CAC ID card reader or a fingerprint reader require that the Extensible Authentication Protocol is used as this provides the extra commands needed to communicate with a reader. Biometrics is not used on its own, rather is the second of a multi-factor authentication solution adding an extra tier to security on top of the username and password (which together form one factor of security).



# **ID badges/RFID badge**

These serve two purposes. Where a CAC card is used, the chip inside the card can contain identifiable information in the form of a certificate file used for authentication. The outer shell can be used to contain a magnetic strip with code to allow access to some doors more generally across the site, and also a photo ID, name, position, and security level for other security staff to read, to validate identity. A radio-frequency ID badge will send a short-range code signal to a receiver on the door allowing access through the door without having to swipe the badge.



# Key fobs

An alternative to an RFID badge is a key fob. This is a short-range NFC device giving a wireless signal with an ID number which, if correct, will open the door, although standing around outside a locked door trying to guess an ID number through a brute-force attack on the lock (using a Wi-Fi cracker) will look suspicious!





# Smart card

A plastic wallet card containing an integrated circuit housing a certificate file used for authentication is referred to as a smart card. These are widely used by retail outlets for loyalty schemes, and are also embedded into credit and debit cards allowing NFC authentication to pay for goods at a till.







# Tokens

In broad terms, any physical object given to identify the user who has access to it is referred to as a token. For example, if you enter the EuroDisney theme park, you receive a wrist strap that is color-coded. The color of the strap used is changed regularly so that security staff know that your strap is valid. A token therefore is anything that identifies that you have already been security checked and are allowed onto the premises.

From an IT perspective, a token is a file sent across the network and attached to the user's account for the duration of your active session. Kerberos is a two-stage process - once you have been authenticated you receive a session token, also known as a **ticket-granting ticket** that allows you the right to ask for further tickets specific to access a particular role on the network.



# Privacy filters

Also referred to as a **glare guard**, this polarizing mesh fits in front of the monitor to only allow the end user to view the screen by sitting directly in front of it. Any light escaping from the screen at an angle relative to the screen will be blocked through polarization, so anyone who is standing next to the monitor cannot see any data on the screen. Whilst not a perfect solution, they are part of a wider strategy of physical devices that can help against shoulder surfing. Open-plan offices often arrange the desk furniture into cubicles to ensure that only one person could, or should, be next to the desk at any one point in time.



# Entry control roster

A guard can have a register of known staff allowed access to a resource, or area of the network. Anyone attempting to access the zone will be checked and if their name is not on the roster they will be denied access.



# Digital security

In this section we are going to identify some of the software measures we can take to protect our systems adding additional layers of security.





# Antivirus/anti-malware

From an IT perspective, we can monitor and protect from both malicious and non-malicious network interference by the use of software-based applications that perform real-time protection from a potential attack. These are broken into two categories:

- **Intrusion Detection Systems (IDS):** These monitor unusual activity and record it into a security event log, but do not stop the attack from happening. They are used as part of an evidence-gathering solution after an incident has taken place to identify what the scope of the attack was and hopefully where the attack came from, showing the weakness in the network security.
- **Intrusion Prevention Systems (IPS):** These are more secure but require a great deal of system resources. Every file in use in memory is scanned against a dictionary of known virus signatures. This can be set to constantly scan (known as **real-time protection**) and also to scan a file when the end user has requested to open and access it. The file is scanned before the file is opened, so it will delay the opening time by a few seconds. Common IPS systems used are Microsoft Defender, Sophos, McAfee, or Norton.



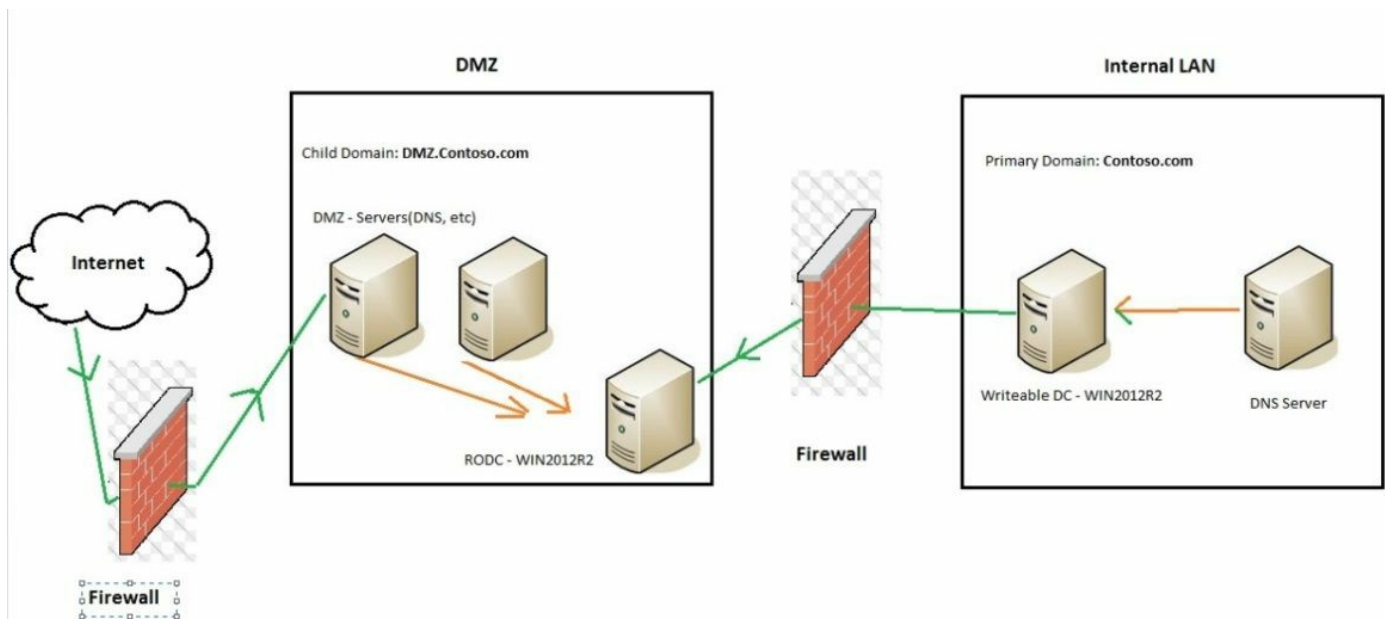
Remember that Defender is installed on Windows systems by default. If you install a third-party application such as Sophos, you will have two IPS systems in place on a client PC which will significantly slow down system resources and may be unnecessary. The Vista version of Defender only protected against malware and was not a full anti-virus application; however later versions are more secure.

A client-side software application that prevents any kind of digital attack or intrusion is known as a **Host-based IPS (HIPS)**. If it only monitors it is a HIDS. Network-facing hardware offering security protection are referred to as Network-based IPS/IDS, so NIPS and NIDS.



# Firewalls

There are at least two firewalls in place on the network. A hardware firewall is used near the edge of your network to block a large number of ports, only allowing significant types of data into your network. The hardware firewall is an expensive piece of kit normally found in the main distribution frame and screens all traffic. You can set it to create a logical semi-secure, semi-public area called the **perimeter network/Demilitarised Zone (DMZ)** where certain applications to be accessed by people accessing the network from the internet can get access to resources without gaining full access to the domain. Often a second hardware firewall is set between the logical partition of the DMZ and the domain to further screen data.





# User authentication/strong passwords

To avoid a brute-force or rainbow attack, we can set in Active Directory the number of times a user can try to log in before their account is locked. Once locked there will be a lockout for a period of time, then a further period of time before the account will automatically unlock. The administrator can unlock the account manually through the **Active Directory Users and Computers Management Console**. Also this action can be delegated to a team leader who can use the Active Directory Administrative Center to do this.

A strong password is defined as more than eight characters and also a combination of letters, uppercase letters, numbers, and symbols.



# Multi factor authentication

As previously discussed, multi factor authentication is the process of having to meet two or more authentication criteria to be able to obtain access. One interesting variant of this is the **Two Man Rule** authentication system to protect against one person taking a major decision which may have a significant impact. An example may be the case of a missile control launch bay where two men, both with their own separate identification codes and keys, need to agree to perform a series of actions to release information needed to go ahead with the planned event. This is to prevent one person from having too much power and thereby making significant decisions that could affect the wider workforce. In the case of a missile launch system, both men would need to agree to go through the opening process. Locks are deliberately placed too far away within the room for one man to reach over and operate both keys at the same time.



According to the US Air Force Instruction (AFI) 91-104, The Two-Person Concept is designed to prevent accidental or malicious launch of nuclear weapons by a single individual.





# Directory permissions, access control lists, and the principle of least privilege

The file and folder access is based on one's user account within Active Directory. If you are a member of a group and the group is stated in the **Access Control List (ACL)** for the folder, then because you are a member of the group, you obtain access at that level of security. If you are named on the ACL, your explicit permission overrides the implied permission, so you will obtain a different level of access based on the fact that explicit permissions trump implicit permissions.

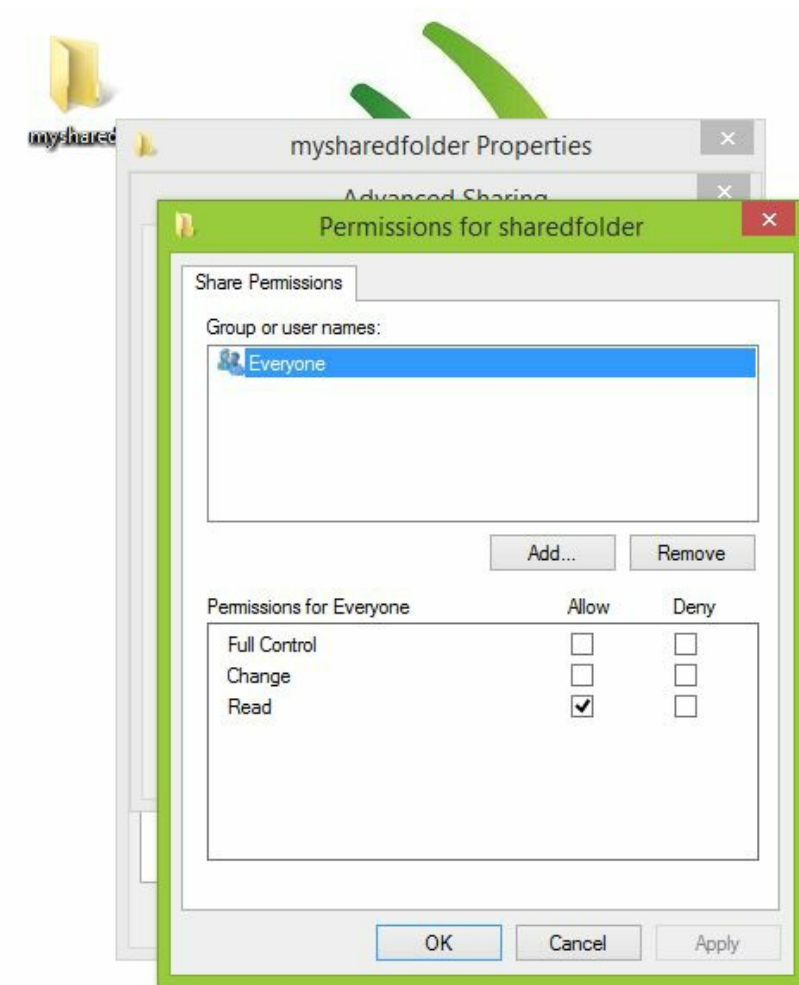
The Microsoft security model is based on the **principle of least privilege**. This is a change to the older model used in Windows NT systems, referred to as the **principle of most privilege**. With PMP, everyone has access to everything until an incident occurs, at which point, the affected user's account is restricted. This does not stop an attack or misuse of privilege in the first place. The principle of least privilege model does just this--each user's access is limited to the bare minimum needed for the user to do their job. If they need additional access rights, these need to be requested through a change management process.

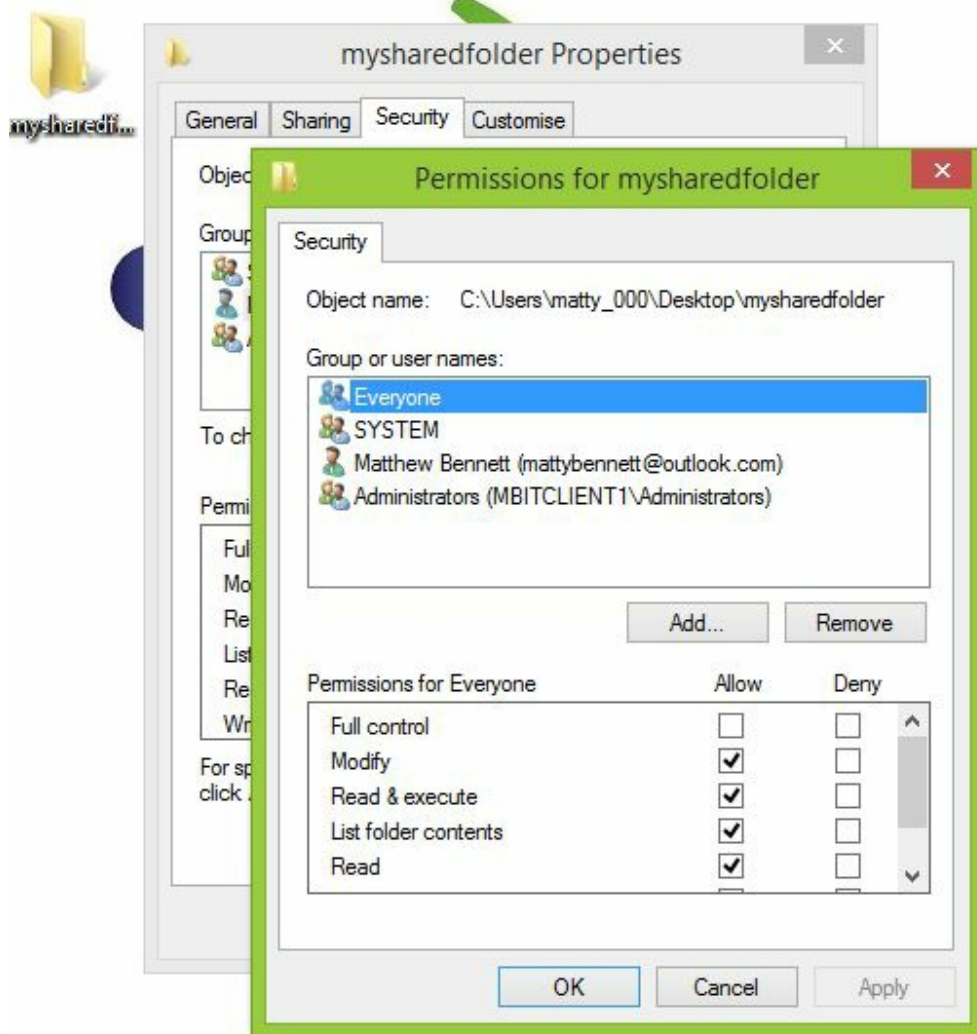
Within one ACL are two columns: Allow and Deny. The PLP model dictates that you should check the box with the higher security permissions that you would like the user, or group to have. The security actions are in order with the most powerful (full control) at the top of the list. Most users have Modify rights to a folder (one following full control), which allows a user to save to a folder, but not to take over ownership of the folder. The folder owner can also control the ACL list and eject other users from the list, thereby restricting access. This is why only administrators should have ownership rights. Ticking the highest security privilege will also enable all of the other actions permissible following it on the list.

There is also a Deny column. If a Deny action is ticked, Deny trumps Allow at that security level, so if both Deny Modify and Allow Modify were both ticked, Deny Modify would win and all of the other settings below it are also denied.

If the resource is being accessed across a sharing address (for example, an UNC path such as `\\server01\sharedfolder`) then the share itself has a separate ACL. Both lists apply and are the most restrictive overall when the NTFS and sharing ACLs are combined. If a user has Read access from the share ACL and Modify on the NTFS ACL, then the user

effectively has Read access when accessing the resource through the share UNC path. However, if the user is physically sat at the PC where the folder is shared and accesses it through a drive letter (for example, `C:\mysharedfolder`) then only the NTFS ACL list applies. In the preceding scenario, the user will have Modify rights.







# VPN

A **Virtual Private Network (VPN)** is a secure, encrypted tunnel through the existing network infrastructure and beyond in to the public internet. It is designed to create a secure connection between two endpoints on the network, also to allow other devices and staff working away from the office to VPN into the network using a VPN tunnel.

Early systems such as Windows Server 2003 and 2008 used the **Point-To-Point Tunnelling Protocol (PPTP)**. This is an OSI layer 3 protocol that allowed routers to check the packet being sent and, if necessary, open the payload, then re-encrypt it. The problem with this is that the internet is effectively just a bunch of routers, most of which are outside of your control. They potentially could contain port mirroring (so packets could be copied) and could decrypt the packet before it is sent on (similar to a man-in-the-middle attack). Also PPTP is an edge-to-edge solution - the tunnel ends with the edge router allowing access to the domain. If you are connecting to another company's domain, other staff within that company are able to see the packets sent to the end PC because the packets are sent between the edge router and the end user PC unencrypted.

In contrast to this, the new layer 2 topology protocol operates at OSI layer 2. It is a switch thing; therefore routers cannot inspect the payload, only forward the traffic on. This gives us an unbroken 'end-to-end' encrypted tunnel.

Added to this, we separately encrypt the IP packets sent through the tunnel using the IPSEC protocol. This can accept IPv4 or IPv6 packets (although we typically configure for IPv6). IPSEC requires either a pre-shared key or certificate to be in place at both ends of the tunnel.

A VPN profile is made in the normal way from the Network and Sharing Center, listing the endpoint and providing authentication information needed to establish the link in the other network.

← Settings

— □ ×

⚙️

VPN

VPN connections

## Add a VPN connection

VPN provider

Windows (built-in) ▾

Connection name

Server name or address

VPN type

Automatic

Point to Point Tunneling Protocol (PPTP)

L2TP/IPsec with certificate

L2TP/IPsec with pre-shared key

Secure Socket Tunneling Protocol (SSTP)

IKEv2

Save

Cancel

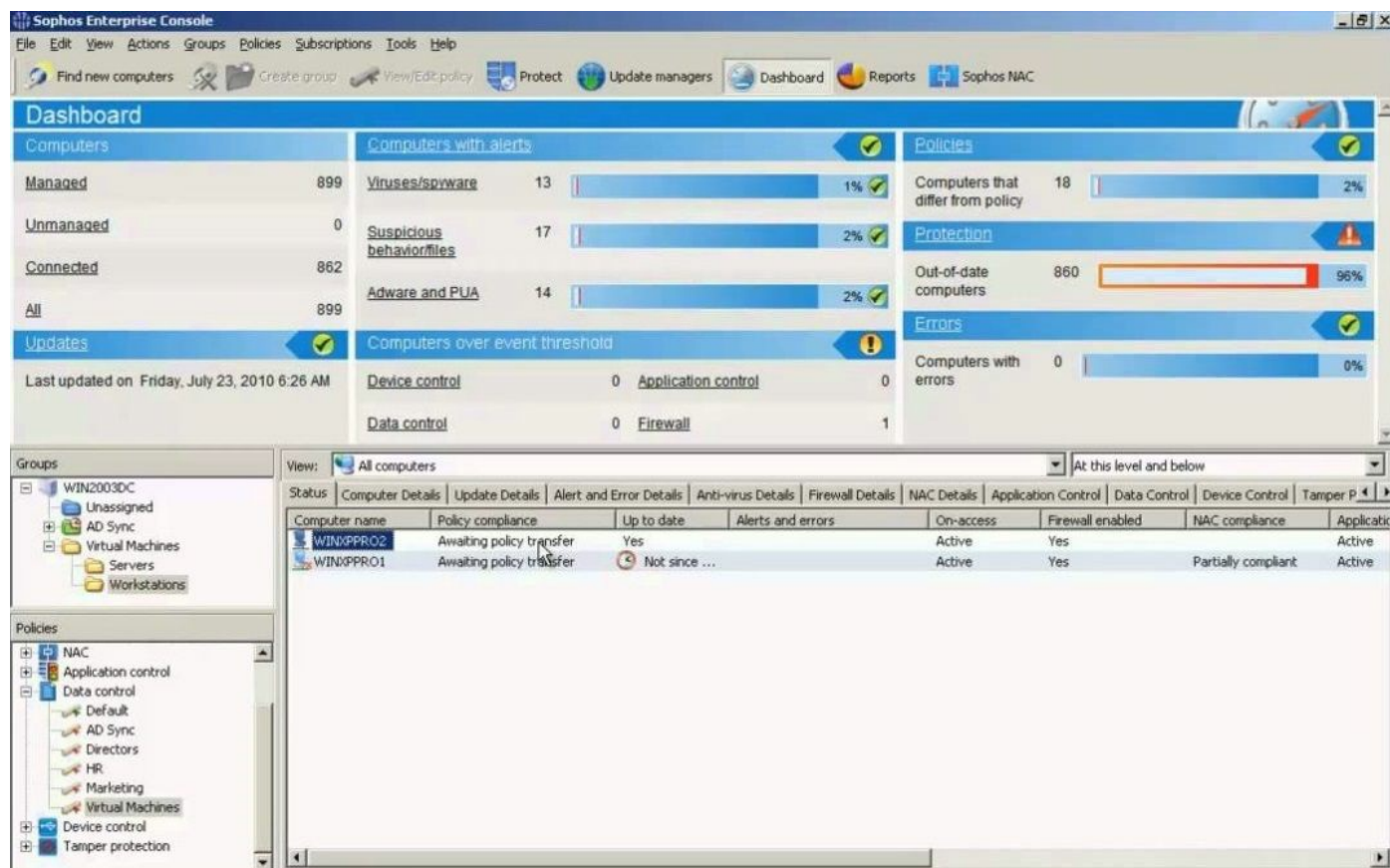
Network and Sharing Center





# DLP

Data loss prevention software detects any possible data breaches or remote commands to delete data from the network. It monitors and then blocks deletion commands whilst the data is in use, in transit, or at rest. It is designed to also prevent sensitive company information from leaving the network and being accessed by a third party outside of our control. Some host-based intrusion prevention systems, such as Sophos, will first check that the data move request is legitimate and has come from a trusted source before the action is performed.





# Disabling ports

Earlier we discussed that both hardware and software-side ports can be triggered to be opened by applications. All except the standard commonly used ports should be closed and only opened when needed. The process of disabling ports is a significant step to network security hardening.



# Email filtering

Certain emails may contain key phrases that indicate that they may be unsavory and not relevant to our business. These are typically captured by our junk email filters; however, this looks against a dictionary of common words but may miss some emails which 'slip through the net'. Our Exchange server can be further trained to root out emails from a specific address, or contain a certain phrase, or keyword. Each keyword is graded and based on the index number given to the email. A manual dictionary of good words and bad words can be developed over time, so that you can train the email server to reject (or place into a spam folder) certain emails before they reach the end user.



# Trusted/untrusted software sources

Filtering email, however, is not very useful when used against content within a phishing email, as the email has been made to look as legitimate as possible, so keywords will allow it through. The giveaway that a phishing email is a scam will actually be that the hyperlinks found within the email will not take the user to the same domain as they expect. The user will instead land on a collection webserver which will register the IP address used by the end user. As the active IP address is now known to the attacker's system, it may in turn lead to other cyber attacks, such as a ransomware attack aimed at that domain, or a file may be downloaded to the end user which is in fact a Trojan.





# User education/Acceptable Use Policy (AUP)

So how can we overcome this? The biggest problem is the current way most enterprise-level organizations operate. They are highly-compartmentalized, so an individual knows their job well, but has no interest in anything outside of their job. To them, IT is just a tool in the same way that a pen should just work as it is expected to, otherwise it will be discarded. This is why a large number of end users are negative towards IT problems and reluctant to change practices due to a lack of understanding that these problems are indeed relevant to them.

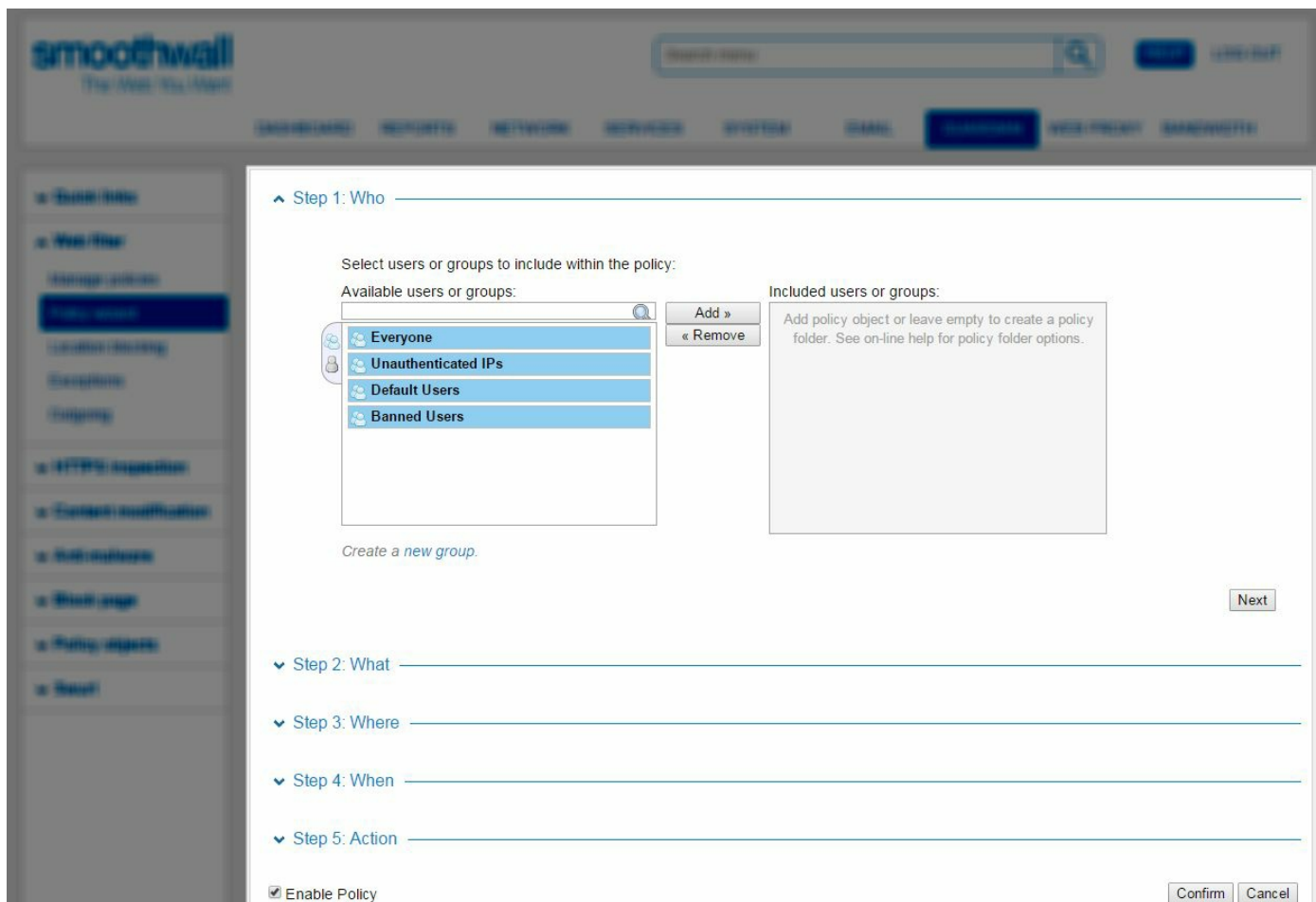
So how do we make them listen? Two ways--education, and enforcement. There is a key motivation for senior staff, such as directors, SEO, SIO, and HR management, to recognize that if they are to attain ISO Data Standards that their IT staff are qualified to hold the position they have. This is now measured through vendor training, such as the CompTIA A+, Network+, Security+, MCSA, MCSE, MCSA, Cisco CCNA, CCNP, and so on. These training qualifications are tested by exam, are not easy to achieve, and demonstrate that you are experienced.

Sorry? Yes--you heard me right. The A+ is not easy. You will pass it if you remember all of the content from this book, but it is a challenge and deserves respect. Once you pass, you equally will be respected because of your achievement.

So, training is critical.

Also, by putting into practice an AUP, we stop the free-for-all mentality the end user may have by treating your delicate and precious network as if it is a home PC to be used as they want. Certain external sites may be damaging to your network and other resources will damage productivity as your staff will not be working as they should be. For example, some companies list Facebook within their AUP as it has the potential to be a great marketing tool, but also can affect productivity as staff can become distracted by personal information, or even trivia.

Through screening out external sites that may harm productivity, we are able to keep the workforce focused. However, access to resources may need to be adjusted as some teams (for example, Marketing) may need access to these for legitimate reasons. This requires a **blacklist/blocklist** and **whitelist** strategy that is tiered to specific AD groups.





# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Physical Security Prevention Methods (6:44):** <http://www.professormesser.com/free-a-plus-training/220-902/physical-security-prevention-methods/>
- **Digital Security Prevention Methods (13:34):** <http://www.professormesser.com/free-a-plus-training/220-902/digital-security-prevention-methods/>
- **Security Awareness (2:46):** <http://www.professormesser.com/free-a-plus-training/220-902/security-awareness-3/>



## **902.3.3 Compare and contrast differences of basic Windows OS security settings**

In this section, we will look again at file permissions as well as the security levels and usage of each type of account. We will also revisit the disk-level and file-level encryption systems used.



# User and groups

Active Directory provides different groups with different security levels which provide different levels of access to the system resources. A user, or computer account (A) is added into a group (global, universal, or domain local) in order to simplify administration. These groups are then added into an **Organisational Unit (OU)** to which group policy objects (policies) are applied.

The AD policy structure is remembered with the acronym: AGUDLP

- **Administrator:** A user with administrator-level security has unfettered access to make system-wide changes. They can install, repair, change, and uninstall software, but also make OS configuration changes. Microsoft advises that you should never log in with the administrator account. Instead, log in with a standard user account and either use the run as option to start the application in another context (for example, for PowerShell or command consoles where the actions you are going to perform will make significant changes to the system). Using the `Run As` command, you will run the application as the administrator, exposing only the one application and leaving the main session still secured. If you are hacked during the session, the hacker can do very little as User Account Control will stop them.
- **Power user:** This group was initially created to allow Windows 3.1 users the same access rights in the later Windows NT system. With slightly more access and control than a standard user, any member of the power users group can change COM object registrations, change file associations so that a file type is opened by an alternative application, change elements on the start menu, install and configure printers, modify a hardware driver used by a hardware component, and modify files in the Program Files directory, but not install applications outright. Finally, power users can modify files in the `Windows\System32` directory.
- **Guest:** There is a fundamental problem with the guest account and so the recommendation is simply not to use it. Any guests to your network should have standard user accounts, but on the domain, in Active Directory, they should be placed into an OU that is heavily locked down, limiting what the members can achieve. If a guest were to make system changes and you were concerned about an action and wanted to know who made the change, what would the event log report? That's right--guest. If you had 20 guest accounts active, who actually made the change? It would be difficult to tell. This is another key reason why we name user accounts.



- **Standard user:** A standard user can personalize their own account and in Windows 10, all of these changes have been split into the new Settings cog on the Start Menu. They can execute previously installed applications and make purchases on the Microsoft store (these apps they can install themselves). They cannot make system changes or uninstall software.



# NTFS versus share permissions

Although we did look at file moves in the Windows chapter, it takes a few goes at actually trying this out for yourself before we can remember if the file is moved or copied, so we will revisit this concept here. There are different behaviors depending on where you are sending the file to. On NTFS volumes, the file's security permissions are changed depending on if you move or copy the file:

"When you copy a file or folder within an NTFS partition, the file or folder inherits the compression state of the target folder. For example, if you copy a compressed file or folder to an uncompressed folder, the file or folder is uncompressed automatically. When you move a file or folder within an NTFS partition, the file or folder retains its original compression state. For example, if you move a compressed file or folder to an uncompressed folder, the file remains compressed. When you move a file or folder between NTFS partitions, the file or folder inherits the target folder's compression state. Because Windows 10 treats a move between partitions as a copy followed by a delete operation, the files inherit the target folder's compression state. When you copy a file to a folder that already contains a file of the same name, the copied file takes on the compression attribute of the target file, regardless of the compression state of the folder. Compressed files that you copy to a FAT partition are uncompressed because FAT volumes do not support compression. However, when you copy or move files from a FAT partition to an NTFS partition, they inherit the compression attribute of the folder into which you copy them. "

Microsoft Official Course 20697-1C Implementing and Managing Windows 10 Student Guide"

- **Allow versus deny:** Remember that the idea here is to use the Allow column first and apply the principle of least privilege. If the user is part of a group then their security level is implied. If the person is explicitly stated and is also part of a group the explicit permission will override the implicit permission. The Deny column can be used to create more interesting combinations by allowing some actions and not others. It should, however, be thought of more as an **emergency stop** button in that pressing **Deny-Full Control** will stop all actions on that folder for that user/group and this may occasionally happen. Your manager alerts you of a problem and you have to protect the resource quickly.

You can also make advanced special permissions, which are a combination of allow and denied actions. When I was delivering an IT apprenticeship my

students had to submit their coursework for marking at 5 pm each day. I had to check that I had received all 20 course works (Word document) files and then place each one into their respective marking folder for my marking team to review. This marking folder was on another network, so I had to move the file to the correct location on the marking team's network, for each student. Before I moved them I gave a final cursory glance through each document, checking that it was complete.



I decided to, as a motivational tool and also to teach professionalism, create an 'Outbox' on my classroom network. This was shared with the students using an advanced 'special permissions' share. The student could copy their Word document into the Outbox, but not overwrite it. They could not open or delete the file once it was in the Outbox, only I could. This got them to check their work was complete before submitting it. As the weeks passed, we compared our results with other classes and other academies and found that we were doing extremely well because the students had taken the care and attention where other students had decided to 'cheat' the system by handing in incomplete work.

- **File attributes:** A file can be set with additional properties, known as their attributes. A file can be indexed (meaning that it will be found quickly if we were to perform a search), it can be encrypted or compressed, it can be archived (all new files that have not yet been backed up have the archive flag set to true so that the file will be captured in the next backup; during the backup process the archive flag is set to false). A file can be set to be hidden, meaning that it will not be listed in File Explorer, or a command console when the `dir` command is run. A file can be set to read-only, meaning that you cannot overwrite it.

Some of these attributes can be set in the file properties windows, from File Explorer, but for bulk changes it is often better to use the command-line `attrib` command to set the flags.



# Shared files and folders

We have already introduced security permissions relating to shares and NTFS folders. This sections will expand our knowledge with other key concepts when it comes to shares:

- **Administrative shares versus local shares:** There is a very slight difference between these types of share. A standard share (a local share) can in fact have multiple share names; you don't have to use the same name as the folder. An administrative share is also called a hidden share. By applying a `$` symbol at the end of the share name, the share will not appear in the network window as a share location, or by the `net` command. All volumes are automatically shared by their derived letter at the time the volume is created, but these are hidden shares. Other notable administrative shares are `ADMIN$`, which provides access to the `C:\Windows` folder, and `PRINT$`, which provides access to the `Printers` folder. The `net share` command can be used to show all shares on the system.
- **Permission propagation and inheritance:** When you create a child folder, it inherits the same permissions as the parent. By blocking inheritance, you can alter the security permissions on the child folder. It is common to do this in situations such as on a file server where you are storing user documents. You don't want the user to manage to go back up through the breadcrumb trail, out of their user area and see the full list of other users, or go into someone else's user area. To avoid this, we create a folder to store all of the user accounts and then block inheritance at this level. We deny folder traversal up into this location. We separately set the child folders (these are created when the user logs on to the network for the first time) so that the user has Modify rights to their own folder and any subsequent folders created in their user area. This allows them to save work into the folder, but not to manipulate the properties further. Here, I am hinting that you do not give them the rights to take ownership; otherwise, they could undo the security you have put in place.



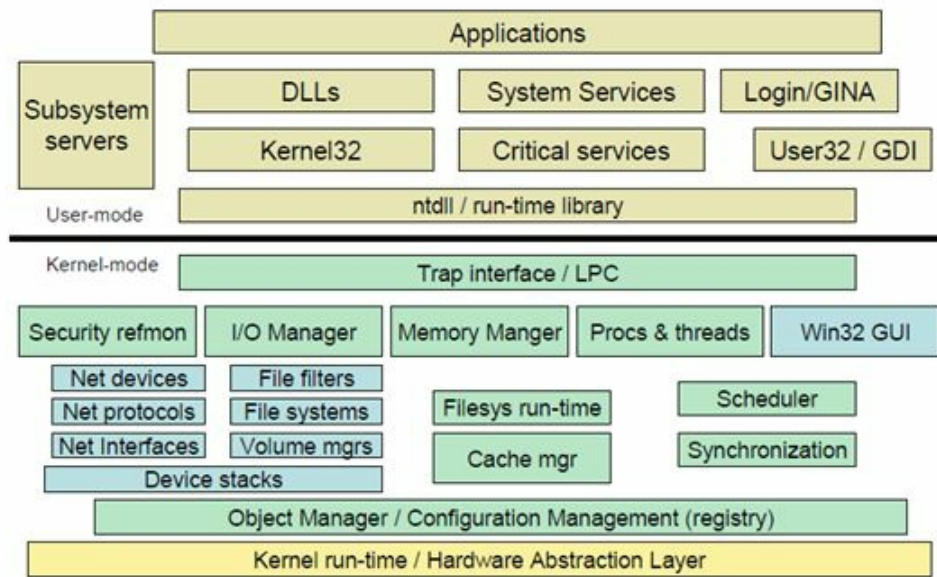
# System files and folders

System files are the various components which when working together form the operating system. These critical files are housed in two locations:

- The Bootstrap files are located in the root of the first volume created. For Windows systems, this is typically the `C:\` drive. These are responsible for low-level access to hardware, further access to the hard drive, recovery of binary data from a hibernate file so that the system can return to a specific point in time when hibernation was triggered, or alternatively load the system. During system load the hardware is audited and an SID number is generated which should match the SID number stored in the registry which was done during the original installation of Windows. As these match, the licence is still OK, so the user is not asked to activate the instance of Windows.
- The core files that make up the Windows system are stored in the Windows folder and also the `system` and `system32` child folders. These are often a list of drivers needed to communicate with various hardware components.
- The `sxs` folder contains copies of drivers and system changes made over time, and also copies of updates installed onto the system. The installer files are also placed in here and serve as a backup, so you do not need the installation media to be able to rectify damaged system files. The **System File Checker (SFC)** is capable of testing each component and repairing it from files stored in the `sxs` folder. Be careful, though--the `sxs` folder will grow to several GB in size and it is tempting to delete it if you are short of disk space. That is not a good idea.



# Windows Architecture



Windows architecture



# User authentication and single sign-on

When a user logs on, the user session is started. The process of authenticating uses either **NT Lan Manager (NTLM)**, on older systems, or Kerberos on modern systems, especially when you are logging on to a domain. For individual standalone PCs and also for work groups, the user account is local to the PC, meaning that the user security object is stored on the local **Security Accounts Manager (SAM)** database. For Kerberos, the user details are stored on the central domain controller as an Active Directory object. Once the session has been started, the user has the right to request further access from the SAM database to access additional components. Every time an application is run, the SAM database has to provide permission to the OS to say that the user account has not changed in some way.

On a domain, once you are authenticated, you receive a **Ticket-Granting Ticket (TGT)**, also referred to as a session token. This allows you the right to request more access to specific resources on the network without having to put your password in every time you want to connect to a resource. A resource ticket is provided to both the user and also the resource itself along with a copy of the TGT. The resource checks that both the resource ticket and TGT match what the user has before access to the resource is allowed. This whole process, where you only need to sign in once, and can then gain access to different resources without being asked to sign in again whilst the session is active, is called **single Sign-On**.



# **Run as administrator versus standard user**

Earlier on, we identified that it is bad practice to sign on as an administrator on the login screen because if the PC was hacked whilst your session was active (or more likely you log in to perform an action, or have to take a call so step away from the PC without locking the screen and another member of staff takes the opportunity to make changes using your account whilst you are away) then the surface area open to attack is the entire session. Instead we ask that network administrators log in with a standard user account and use the Run As option to elevate permissions for the one application only.



# Encryption systems

BitLocker is a full-disk encryption system. The encryption key is in fact a certificate file that can be backed up in Active Directory. The certificate is installed on a Trusted Platform Module chip on the motherboard and this ties the hard drive to this PC specifically. Alternatively, the certificate can be placed on a USB pen drive and needs to be inserted before the hard drive can be used.

The later version of BitLocker can be set to only encrypt the portion of the drive that has been used (the partition). This may mean that access to the data is quicker, if the hard drive is old and has been used to create many partitions which have now been deleted, old data may still reside in those areas of the disk which is not being protected by BitLocker. I therefore recommend that you leave the settings set to full-disk encryption.





# BitLocker-To-Go

A version of BitLocker which will encrypt data saved to a USB pen drive is called **Bitlocker-To-Go**. In essence, it works the same way as the normal BitLocker. A PIN code has to be known to access the pen drive once it has been encrypted, or an encryption key is stored onto the PC. EFS - a much older technology and not as secure as BitLocker because the encryption key used is much smaller. The encrypting file system allows you to encrypt individual files. It is compatible with BitLocker--you can use both technologies. EFS requires that you are using an NTFS formatted volume.



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide.

- **Windows Security Settings (9:28):** <http://www.professormesser.com/free-a-plus-training/220-902/windows-security-settings-2/>



## **902.3.4 Given a scenario, deploy, and enforce security best practices to secure a workstation**

In this section, I want to explain why it is good practice to use some of the security features available to you from both the local security policy list and also Active Directory. These can be enforced across the network to ensure that your accounts are secure but also that users are managing them correctly.



# Password best practices

Here are a few tips and good practice guidelines CompTIA are keen that we as IT professionals follow.





# Setting strong passwords

We don't use a memorable word, such as a child's name or favorite toy as a password because if we know the individual we can work out what the password might be. Instead, we request that such memorable words are salted by adding additional or replacing existing characters with uppercase letters, numbers, or symbols. This makes it much more difficult to guess the password without the use of a Rainbow table where different permutations of the password will have to be tested by the hacker.

Ironially the chief advier who many years ago advised to make difficult passwords which are hard to crack (and remember) has recently relented on the news. He now claims that he was wrong to say this as rainbow tables and brute force attacks can guess a password as easlity as if it was a simply password.



# Password expiration

By forcing the user to change their password on a regular basis means that if someone has compromised their account by learning the password, they would have to start again. By also enforcing a password history, the system will not let the user use previous passwords that have been used, forcing them to generate something new.



# Changing default usernames/passwords

The default for the administrator account is **admin** and the password for the local admin account was set during the installation. Because of this, if the technician did not know what to set the password to, a generic one may be used. It is likely that this admin account has the same password as every other OS installed across the network, so learning this local admin password would be a security risk. If an end user were to log in using a local administrator account, they can circumvent whatever security protections you have put in place on the domain. For this reason, we use a complex password and give this password to the technician to use, but then after the PC has joined the domain, we disable the admin account in the SAM database on this PC. Instead, we add the **Domain Admins Active Directory** group to the **Administrators** group on the local SAM database. By doing this, any member of staff designated as an administrator for the domain will be in the Domain Admins group, so they get admin rights on the local PC. Clever!



# Screensaver required password

I mentioned the scenario where the administrator logged on to the PC to make system changes but had to leave to make a call. Over time a screensaver will start, so that the monitor does not get an image burned into the screen. However, one move of the mouse will remove the screensaver and return us to the active session. If the lock account option is selected, moving the mouse provides us with an authentication box. This stops other people from misusing the administrator's account while they are away from the PC.





# BIOS/UEFI passwords and why autorun is disabled

It is very good practice to stop users from altering the BIOS. Once it is set, you really should not change it as the processor frequencies (for example) are now set to a specific speed and this speed is also known to Windows. If you change the frequency, Windows will try its best to start but may become unstable, but the hardware profile was set during the installation of Windows. Also important is the fact that you can disable USB ports through the BIOS (and other users can switch them back on). Some technicians put resin over the front ports and glue the keyboard and mouse into the only two working ports. Whilst I do not recommend gluing hardware into ports, if the USB device was removed from the port temporarily, other things such as a USB pen drive containing keylogging software, or even an alternative operating system, can then be accessed and used. If a user can access the BIOS, they can enable other ports allowing for even easier access to install a pen drive that is up to no good.

The BIOS also contains a list known as the **boot order**. This defines the order in which the system will try to find the bootstrap files. The system can PXE boot from a network card, or access a bootable CD-ROM, or access a hard disk. We used to leave the settings so that it would try to boot from a CD first. If no CD was in the drive then it would boot from the hard drive next. This policy has changed because the bad guys may also be able to boot from a CD in this case! From Windows 7 and later, the CD autorun feature has been disabled by default to stop people from being able to run without checking what is on the disk first. We now therefore have a separate BIOS password known only to the administration team.



# Requiring passwords

We now can also require that a password is entered before the bootstrap process begins. Both UEFI and BitLocker protected drives have this mechanism ensuring that the user is a known good user who has the right to access the PC, and after all, what better way to protect the PC's data than if it were inaccessible because the PC is off?



# Account management

These are a number of additional restrictions we can set on accounts to ensure that users log in only within certain times of the day, or to certain machines only.



# Restricting user permissions

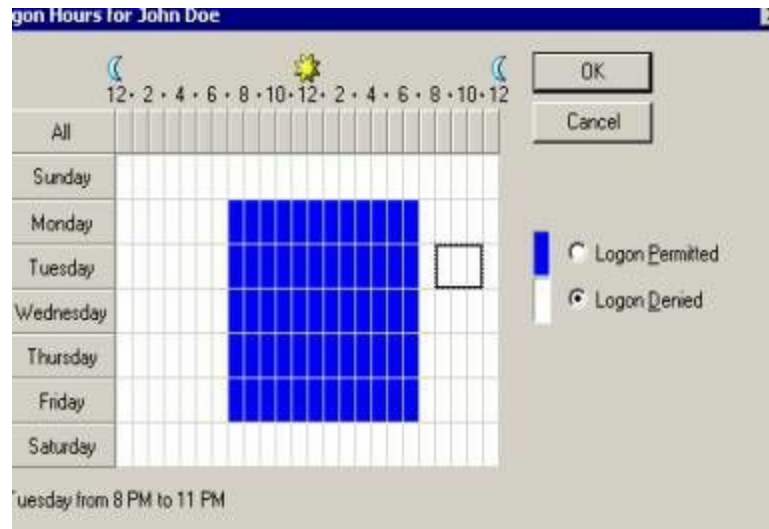
User accounts are restricted based on the Active Directory OU they have been placed into. I design my enterprise networks with OUs to represent different departments. I also use AD Sites and Services to define where my PCs are physically located by creating branch offices and a head office. Through this scoping exercise, we can define **Group Policy Objects (GPOs)** to apply to specific groups of people and computers only. When a PC boots up, it communicates with the domain controller and receives any policy changes. When the user logs in, the same happens and GPOs are applied to the account.





# Login time restrictions

If you know that a user works set shifts, unusual activity such as the PC being accessed by the users account in the early hours of the morning would be suspicious. To stop this, you can set login time restrictions so that the user account can only be used on certain days and within set hours.





# Disabling guest account

I just wanted to remind you that it is not good practice to use a guest account on the network because if the guest were to do something untoward, how would you know which guest it was? Better practice is to create standard user accounts for your guests, but place them in an OU that has tight security on it, so that they cannot make changes to the network, or install files. This can be easily achieved by linking a GPO to the OU.



# Failed attempts logout

To protect from a brute-force attack, or rainbow attack, where different permutations of the password are tried, we can lock the account after a certain number of tries. This then forces the user to get in touch to unlock the account.



Remember, network administrators do not know user passwords. Given the nature of your role, users will suspect that you do have access to it, but in truth you don't need to. You can replace the existing password with a new one you have made up at any time, and you can also unlock accounts by unticking a check box.



# Timeout/screen lock

Within Active Director's group policy, and also for local accounts in the local security policy, we can define how long a user is locked out of their account for. The user will assume that the lockout is permanent and will then call your team to have the account unlocked. You may decide that you want to do this, as this gives you an opportunity to security screen the user before unlocking the account, but normally we don't need to do this. A timeout period can be enforced so that the account unlocks automatically after 10 minutes (this is the default setting). You may decide to do this to avoid the lockout calls. Lockouts are enough of an irritant to train the end user to remember a password.





# Patch/update management

The process of patching the PC can be automated, but best practice is that updates should be approved first before being rolled out across the network. This is done by using a known good test PC in a workbench environment. Expose this to the update first and verify that the update does not have any adverse affects. Then, the update is approved in the WSUS updates list. WSUS will only push out updates at a set time, usually one evening during the week. Microsoft tends to release updates on a Tuesday evening. For home users, this is evident as when they close down their PCs they will be prompted with a message stating that an update is in progress before the system will shut down. This of course depends on if you have allowed the system to automatically install updates, or to download them first and ask for your permission to run the update, or set the Windows update feature to not install them at all.



The action center will report with an alert/red shield if you have disabled updating.



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide.

- **Workstation Security Best Practices (9:12):** <http://www.professormesser.com/free-a-plus-training/220-902/workstation-security-best-practices-2/>



## **902.3.5 Compare and contrast various methods for securing mobile devices**

Moving on from the PC, we are going to look at security features specific to tablets and smartphones.



# Screen locks

Security on our mobile devices features an array of new biometric or password systems which we will look into here.





# Fingerprint lock

A fingerprint (usually of the left thumb) is taken by the fingerprint reader. For Android phones, this is integrated into the central button on the front face of the phone.



# Face lock

Key features of the face are taken, such as the relative distances between the eyes and nose and these features form part of a face recognition pattern. Here, the camera records a picture of your face and uses features to determine that you are the same person. This takes into account makeup, a change of glasses, or hairstyle. The front-face camera is used for this.



# Swipe lock

This requires you to swipe your finger across the screen to unlock the screen. As there is no memorized code or pattern, we deem this to be a very insecure mechanism as anyone's finger will do.



# Passcode lock

There are several variants here. The pattern lock requires that you draw a shape with your finger using a 3 x 3 dotted grid. If the pattern matches the one saved on the profile then you are allowed access. Alternatively, you can enter a four-digit PIN code, or a password. The mobile phone buttons, or keyboard will become visible allowing you to tap in the code or password.





# Remote wipes and locator applications

If your device is lost or stolen, you can contact your provider who will be able to try to locate it, lock it, or erase the data from it. The phone has to be turned on for this to work. As the phone is on, it is broadcasting on the cellular network. The provider can perform a trace to see which cell radio mast it has connected to. This can be triangulated against a map to list where the last signal came from.

My son had a blackberry phone whilst at primary school. The provider was O2. He had to put his phone onto a tray and then collect his phone as he left at the end of the school day. One day, when he went to collect his phone, it was not in the tray. He suspected that another child had stolen it. Later, we contacted O2 who confirmed that the last signal was earlier in the day from the radio mast adjacent to the school. We decided that a more thorough search would reveal it, or if it was an honest mistake the person may return the phone. We also decided against a remote wipe on this occasion as there was a good chance that it was still in the school. The next day we checked with his classroom teacher who had the phone in her desk--my son had handed it into her at a different time in the school day which is why it did not go into the tray with all of the others.

To find an Android phone associated with a Google account:

If you lose an Android phone, tablet, or Wear watch, you can find, lock, or erase it. Find My Device is on by default for Android devices associated with a Google Account. To use Find My Device, your lost device must be:

- Turned on
- Signed in to a Google Account
- Connected to mobile data or Wi-Fi
- Visible on Google Play
- Location turned on
- Find My Device turned on Lost Android Wear devices must also be running
- Android Wear 2.0 and up.



Tip: If you've linked your phone to Google, you can find or ring it by searching for Find My Phone on [google.com](https://www.google.com).

To remotely find, lock, or erase the device:

When Find My Device connects with a device, you see the device's location, and the device gets a notification.

Open [android.com/find](https://android.com/find) and sign in to your Google Account. If you have more than one device, click the lost device at the top of the screen. On the map, look for where the device is. The location is approximate and may not be accurate. If your device can't be found, Find My Device will show its last known location, if available. Pick what you want to do. If needed, first click Enable lock & erase. Play sound Rings your device at full volume for 5 minutes, even if it's set to silent or vibrate. Lock locks your device with your PIN, pattern, or password. If you didn't have a lock, you can set one. You can add a recovery message or phone number to the lock screen. Erase Permanently deletes all data on your device. (It may not delete SD cards.) After you erase, Find My Device won't work on the device.

Find my iPhone for Apple devices: <https://support.apple.com/explore/find-my-iphone-ipad-mac-watch>



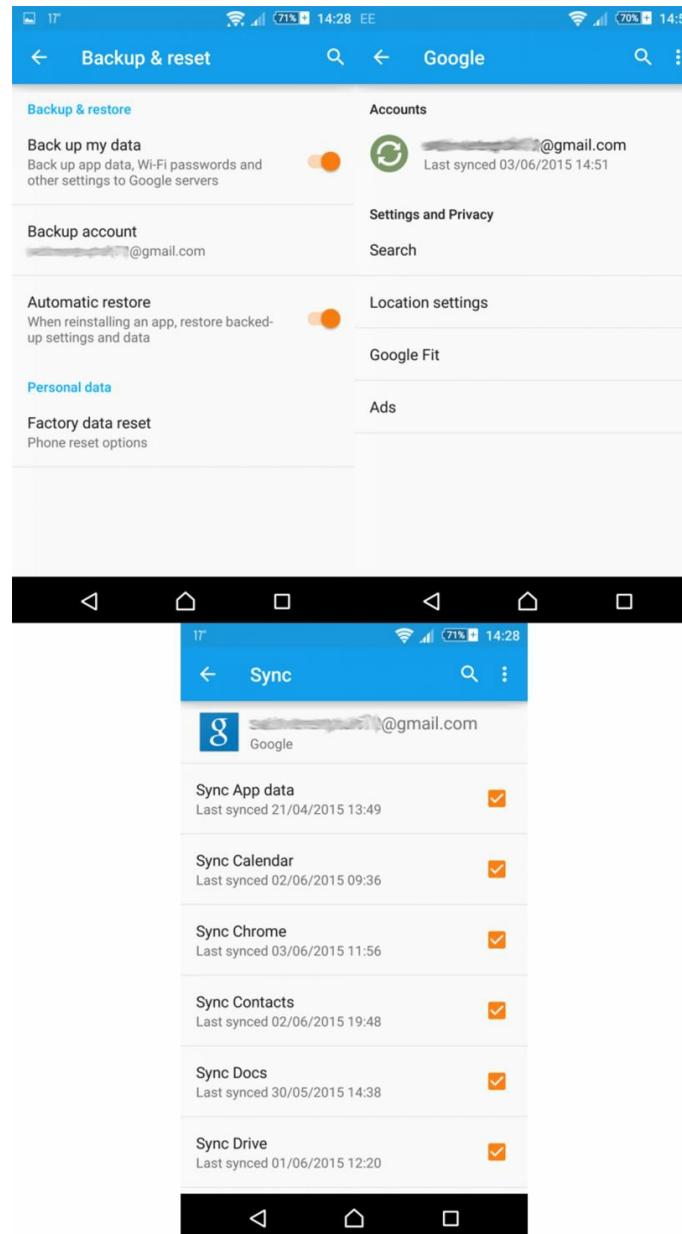
**Important:** If you find your device after erasing, you'll likely need your Google Account password to use it again. <https://support.google.com/accounts/answer/6160491?hl=en>



# Remote backup applications

By far the easiest solution is to associate your smartphone to a Google account. If you navigate to Settings | Backup & reset and then tap Back up my data and Automatic restore, this will backup:

- Google Calendar settings
- Wi-Fi networks and passwords
- Home screen wallpapers
- Gmail settings
- Apps installed through Google Play (backed up on the Play Store app)
- Display settings (Brightness and Sleep)
- Language and Input settings
- Date and Time
- Third-party app settings and data
- For information on Apple backups: <https://support.apple.com/en-us/HT203977>



- **Failed login attempt restrictions:** You can set the phone to remote wipe data, or reset to factory settings if the user has attempted and failed to put in the correct password, gesture, or PIN too many times. First go to Settings | Security | Screen lock. On its own, the OS does not support the feature to perform an action after a number of failed logon attempts but third-party, software such as Locker from Zygote labs, can add this functionality. Here we can add the number of permissible failed logon attempts and also what to do if this number is reached.
- **Antivirus/anti-malware:** Smartphones also need to be protected from virus attacks, especially as devices may legitimately be used as a file storage system to hold company data. If the device is CYOD, then it is a company asset just as any other PC. That means that from a cyber security standpoint, CYOD devices should also receive the same protection as any other piece of hardware on the network. To

be approved for a Cyber Essentials audit, companies have to ensure that CYOD devices also have adequate anti-virus protection. AVG is a common app used to protect phones and is one of a multitude of apps available from the Play Store. The main point here is that it is used to ensure that files remain safe, and also end-user training to ensure that the anti-virus software is enabled and that regular scans are run.

- **Patching/OS update:** Just as with the PC OS, the phone's inherent operating system will need to be patched. Once permission has been given for patching to occur, this is typically an automatic process. More notable are OS updates where the actual version of the OS will upgrade. The process of updating is much quicker than a PC's OS because the footprint is so much smaller.

Android versions are easy to identify, as each is the name of a sweet, or other food, such as Gingerbread, Ice Cream Sandwich, Lollipop, or Marshmallow.

To check for system updates manually:

1. Open the Settings menu for your Android.
2. Scroll to the bottom of the menu and tap About device.
3. Tap System updates.
4. Tap Check for update.
5. Tap OK if asked to confirm
6. Wait while your device checks for updates.
7. Tap Download or Yes if an update is available.

- **Biometric authentication:** As discussed earlier, biometric authentication can be used either by the fingerprint reader, or the camera using facial recognition.
- **Full device encryption:** With iOS v8 and later, everything on the whole device is encrypted. The encryption is based on the passcode used to access the device. Android can also support this feature but it has to be enabled, whereas Apple has this enabled by default. For Windows phones, this is enabled by using **Exchange ActiveSync**.
- **Multifactor authentication:** A series of different authentication methods can be used in a series to increase the complexity, but also the security of the device. Authentication types are broken down into three categories--something you know (password), something you have (key fob), and something you are (position in the company).
- **Authenticator applications:** I regularly use one of these apps to provide security to my Microsoft account and related websites. If I am accessing a website such as

the Microsoft's courseware download center on a PC that is not my usual one, I have set the account to request an authorization code be sent to my phone. The code appears in the app on my phone and I check that the code matches before then pressing the Allow button on the app. This sends a signal back to the Microsoft server that I personally approved access to this resource. If I were to add my Microsoft account to a local login on a new laptop, this also will occur. This is another example of second-factor authentication.

The authentication code is pseudo-randomly generated and typically is a combination of letters and numbers.

- **Trusted sources versus untrusted sources:** A trusted source is typically a website or app provider that is known to the user and the user is making a decision to believe that the provider is trustworthy. For Apple, all applications are installed from the App Store and have had to go through a rigorous quality checking procedure before they are allowed to feature on the store for users to download.
- **Firewalls:** It is not common to see a firewall on a mobile device, rather when you connect the device via a Wi-Fi access point the firewall is on the access point, or deeper into the network. This can be dangerous for the network as you really would like mobile traffic entering the network through the front door, as it were, through the main distribution frame and the vast array of security we already have in place. We therefore segregate a separate logical network (a **sandbox**, or **public Wi-Fi**) which allows access to limited local resources available as part of the DMZ. Anything else has to be navigated to via web links, therefore forcing the phone effectively to 'come in through the front door' after all.
- **Policies and procedures:** The main problem with the CYOD model is that the asset is not the user's own, so they will expect the IT team to maintain it. This normally means fixing it when it is broken. Quite often, end users will think that the mobile phone is out of scope of an existing policy document signed for PCs across the network. For this reason end-user training is vital. With the BYOD model, the company cannot enforce that the device is updated and clean from viruses, which is why some companies prefer to separate the resource from the phone, as discussed in the Firewalls section.





# BYOD versus corporate owned

BYOD versus CYOD. A key challenge for network managers pertinent at the present time is the concept of **Bring Your Own Device**. This is the process of allowing your employees to connect devices (irrespective of the make or model) to install a certificate file you have provided for them to use, which effectively joins the device to the network. This provides the user with functionality of network resources but raises issues around device and network security, and also data security. For this reason, manufacturers are now making it very easy to allow the user to casually join and disjoin a domain at the press of a button. This is good for the user because when the device is joined it has to ascribe to any policies listed by relevant GPOs already set up. Until the device is disjoined, these policies will apply, even when away from the physical corporate network, which may limit the normal functions of the device (for example, a smartphone).

In contrast, **Choose Your Own Device** is an alternative where the device is owned by the company and given to the staff member as an asset to use. The company typically buys in bulk and any servicing is managed by the in-house IT team. Typically, one make and model is purchased so as to simplify IT servicing and standardize the device across the network, minimizing potential issues that may occur. Installation of files or certificates would clearly affect the phone which may be locked down and only capable of certain services. Misuse of the device, such as for personal reasons (for example, accessing personal emails) may not be permitted on such devices.

Enterprise Management solutions such as InTune or System Center are widely used across organisations to ensure that devices are compliant when connected to the network. With this and also Network Policy/System Health servers the network can be protected from dirty devices attempting to connect.



# Profile security requirements

Even if we use BYOD, you as a network manager, need to be able to administer the device and ensure that it meets standards before it can access your data. We use for this a Mobile Device Manager application, such as Windows Intune, which is typically used to refresh, update, and ensure compliance on PCs, Apple devices and a whole range of smartphones and tablets. Intune is the web, cloud version (and lighter version) of System Center and is capable of batch processing as well as enforcing security standards across the network. Intune is also commonly used by administrators to batch-fix a whole variety of machines on the network, triggering updates in one go.



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide.

- **Securing Mobile Devices (9:00):** <http://www.professormesser.com/free-a-plus-training/220-902/securing-mobile-devices/>



## **902.3.6 Given a scenario, use appropriate data destruction and disposal methods**

In this section, we will consider how to destroy and to recycle hardware safely. I will indicate some of the correct procedures to follow.





# Physical destruction

Sometimes the most drastic solutions are the obvious but definitely the most effective. As a final resort companies may choose to physically damage or render inoperable the storage device ensuring that data cannot be retrieved.

- **Shredder:** Believe it or not, you can purchase industrial-grade chippers, similar to wood chippers which are especially designed to chew up hard drives. They are expensive and not often used; however, the sensitivity of your data may require that the hard drive cannot be recovered. This will certainly do the job as you are left with tiny metal pieces and it is impossible to reconstruct a working hard drive from them.
- **Drill/hammer:** A cheaper alternative to the chipper is a drill, or hammer. With a hammer you can break the outer casing and possibly bend the platters; however, by drilling holes through the platters the data is unreadable. Normally the act of breaking open the case and allowing the air to enter the chamber is sufficient to render a hard drive inoperable, but it's always good to ensure that it will definitely be.
- **Electromagnetic (degaussing):** A degausser is a strong iron electromagnet that creates a very strong electromagnetic field. These are often used with backup tapes, or video tapes where the tape is planned to be re-used but you want to completely erase all data from the tape first. With hard drives, however, the electromagnetic field not only resets the platters but also wipes the firmware on the disk controller card located on the hard drive and by so doing renders the hard disk useless.
- **Incineration:** The ultimate strategy would be to incinerate the drive. This would melt the components to bare metals, clearly rendering the hard drive, well let's just say that you couldn't reconstruct it.
- **Certificate of destruction:** Most of these devices are probably not available to most companies, so there are third-party data destruction companies who will take your drives and dispose of them for you. They will issue you with a certificate of destruction as proof that the drive has been disposed of. This is useful for auditing purposes as you may need to prove that the hard drive has not been stolen, but was in fact destroyed on a particular date.



# Recycling or repurposing best practices

Rather than destroy the storage device, you may simply want to wipe and reformat it so that it can be repurposed. We will look at how we can recycle storage hardware here.

- **Drive wipe/low level format versus standard format:** If you want to continue to use the hard disk, you could just re-format the partition. A low-level format sets all of the bits to 0, then all of the bits to 1, then back to 0. This readies the drive for use.



If you work for a company with a Microsoft Enterprise account, you will be able to download the Diagnostic and Recovery Toolkit. This is a vital ISO file you can burn to a DVD and use as a swiss army knife. It contains a suite of programs allowing you to reset SAM passwords, but more importantly to also perform a low-level format, or to undelete files from an existing partition. Information about DaRT is available here: <https://technet.microsoft.com/en-us/windows/hh826071.aspx>

If you don't have a Microsoft Enterprise account, you could instead use a Linux distro available with similar tools known as Hiren's Boot CD. <http://www.hirensbootcd.org/download/>

Users cannot perform a low-level format. The OS format option restructures and readies one area of the hard drive (a partition) to be readied to receive new data. In truth, this area is not wiped; only parts of it containing the new format information (known as a **quick format**, which is the most common). If you are keeping the same block sizes and format type (for example, NTFS) then you may still be able to use undeleted software to retrieve old files. This clearly is a security risk, so I would advise low-level wiping a hard drive before it is re-commissioned.

- **Overwrite:** The process of adding new data over an existing block thereby wiping over what was there previously is referred to as overwriting. There is no guarantee that the new data is any bigger than the old data and so parts of the old data can be recovered using a low-level reader, or an undeleted program on the areas that were not wiped over with fresh data.

In July 2013, in the UK National Health Service Surrey, they found that they were providing these hard drives to be destroyed by a third party, but



they really weren't destroying them. These drives contained patient records, and although the Health Service was provided a certificate saying that the drive was really destroyed, in fact, the drives were sold on eBay. Someone bought the drives, found the patient records, and contacted the authorities. And unfortunately, the Health Service was fined over £200,000.

Source Professor Messer: <http://www.professormesser.com/free-a-plus-training/220-902/data-destruction-and-disposal/>



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide.

- **Data Destruction and Disposal (4:13):** <http://www.professormesser.com/free-a-plus-training/220-902/data-destruction-and-disposal/>



## 902.3.7 Given a scenario, secure SOHO wireless, and wired networks

There are a number of specific things you have to do to secure a wireless access point which apply to both the domain and smaller networks, such as a **SOHO network**. In this section, we will look at some of the security actions you should take and explain why they are important.





# Wireless specific

In this first section, we are going to concentrate on wireless-specific elements we can configure to harden our wireless access.



# Changing default SSID / Disabling SSID broadcast

The **Secure Station Identifier (SSID)** is the name by which the access point is known. For a Sky home router that would be **SKYxxx** (where **xxx** is a combination of hexadecimal numbers). You might want the SSID to be something more memorable and in keeping with your company, such as the company name and then a number to indicate which access point it is. A SSID scan will show a variety of SSIDs in the local area, omnidirectional from the wireless device of up to 150 feet.

Once you have set up a profile on the connecting device, you will want to deter unknown and untrusted sources from accessing your network through this Wi-Fi access point. To do this, we simply hide the SSID so that when they run a scan, the SSID does not appear in the list. When you create a wireless profile, you can add the SSID in manually, so new users who need to access the Wi-Fi access point legitimately can be provided with the SSID once you have checked that they should be allowed access.

It is good practice that as soon as the Wi-Fi access point is set up, the SSID is hidden.



# Setting encryption

Wi-Fi access points can use a variety of encryption systems ensuring that the radio data packets, if intercepted by another third party also present within the access point's range, would be meaningless. There are encryption options such as WEP (Wired Equivalent Privacy), but more commonly we will use WPA or WPA2 (Wi-Fi Protected Access). WPA is used as a bolt-on to WEP, not a replacement, as WEP is flawed and not particularly secure on its own. In fact you can download WEP cracker apps from the Android store, which will crack WEP security in a matter of minutes.

WPA uses the 802.11i standard. Where WEP used a static 64 or 128-bit encryption key, WPA uses **Temporal Key Integrity (TKIP)**, where the key changes for every packet sent. WPA also includes a message integrity check so that if the packet has been altered and resent by a man-in-the-middle then we will know as the packet checksum will not match up with the data sent.

WPA2 allows us to use the **Advanced Encryption Standard (AES)**, also known as the **Rijndael** (pronounced: Rhine-Dale) specification. The Rijndael key is 128, 192 or 256 bits in length, so is very secure. In practical terms, this means that we can have a very secure network using the encryption standard also used to encrypt hard drives! (for example, BitLocker and TruCrypt both also use Rijndael).



# Antenna and access point placement

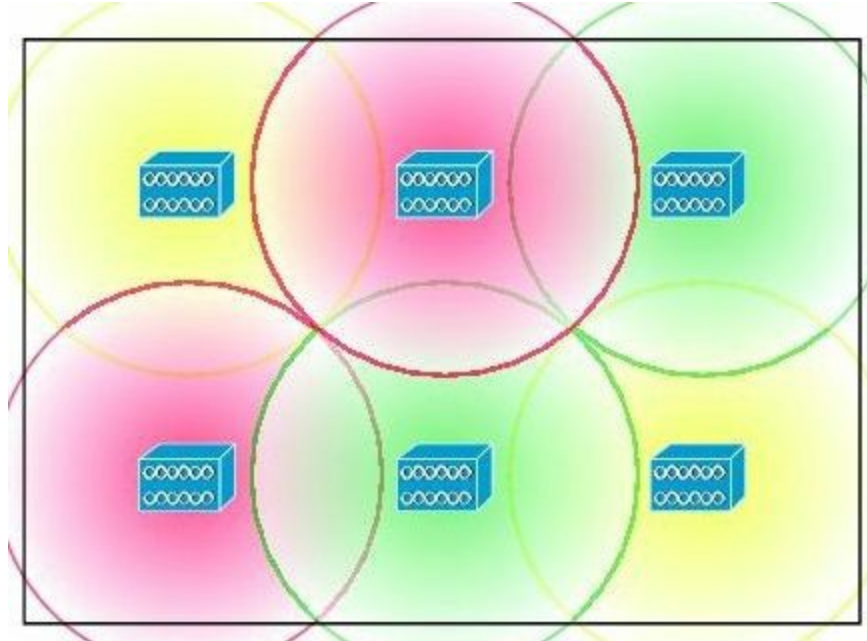
A standard Wi-Fi access point has an omnidirectional area and a range of 80-150 feet, depending on the protocol used and the power of the antenna. Devices within this range can connect to the AP without issue. Devices beyond the range, where the signal strength is between 50-60%, may receive some packets but get a lot of errors and dropped packets. APs are placed to be slightly overlapping and for the range not to bleed out of the building.





# Radio power levels

It is good practice not to run your antenna at full power, but rather to alter the power level to reduce the size of the cell so that you can ensure that the signal does not bleed through an exterior wall and only just overlaps its neighbour cell.





# Wi-Fi Protected Setup (WPS)

This operates in a similar fashion to Bluetooth pairing. Created by the Wi-Fi alliance in 2006, the aim was to easily add new devices to the network without having to set up complex profiles by sending the configuration information out from the Wi-Fi access point to the new PC. A later variant of WPS uses a PIN code (seven digits); however, this PIN is susceptible to a brute-force attack. Other models use either a USB pen drive with specialist software provided by the manufacturer to establish the link, or the push-button method. Here the new PC has a WPS-enabled Wi-Fi network card with a WPS push button. You press both this and the WPS push button on the router. Both devices send a handshake signal and the configuration is sent to the PC. The handshake will send out for up to 2 minutes, allowing you to physically move from the one device to the other.

This following is a list of all of the common security and hardening practices you are expected to carry out on a Wi-Fi router:

- **Change default usernames and passwords:** On a standard SKY router, the username and password are `ADMIN` and `SKY`. It is therefore highly advisable to change this admin account's username and password to something you can secure.
- **Enable MAC filtering:** The MAC address is the physical address of the network card. By only allowing approved MAC addresses on your network, you can block any other address that is not part of your existing list. Devices trying to connect to your router/access point will be ignored. This only works so far--if the hacker is able to determine a known good MAC address (Cain and Abel will be able to sniff all radio communication within range and report back on the MAC addresses in use), they can then MAC spoof by changing their NIC's MAC address to a known good, therefore bypassing the list. MAC filtering is definitely worth doing but is not a complete solution on its own.
- **Assign static IP addresses:** It is important that the router's IP address does not change. If it does then other devices will not be aware of the change and not be able to find it. For this reason, we assign static IP addresses for entry points, domain controllers, DNS and DHCP servers.
- **Firewall settings/disabling ports:** The firewall should block most ports other than essential ports for common services. We limit inbound traffic to only specific types of traffic, as we covered in the 901 section of the book.
- **Port forwarding/mapping:** I have a Dynamics CRM server in my office. I connect

to it when I am away from the office using Port Forwarding. I have a public DNS server with an entry which takes me to my office entry point (my router). When accessing this router using a specific port number known only to me, the router knows to forward the traffic internally to the specific server where my CRM software is installed. As Dynamics CRM is a web-hosted service, I see the web page for my CRM account.

Sadly it doesn't work when the server is turned off. I leave it on standby mode and when I'm in the building can send a **Magic Packet** to the server which wakes up the server. However, to the best of my knowledge Magic Packets are not routable--they only work when I am within the subnet.

- **Content filtering/parental controls:** We can block access to certain websites based on key words within the body text of the web page. Home users also have restriction to certain sites based on the categorization of the website, which is done by my ISP. Sky Broadband Shield is an example of this--any web requests are checked against the content filter settings set within my Sky account. If the site is not part of a known blocked category (for example, gambling sites), then the traffic is allowed. I can, through the Sky Broadband Shield, create my own list of banned sites and maintain this list myself. You can also bypass restrictions for certain sites that you know are safe, or have decided that you would still like to access.

Content filtering is also possible within the individual PC as it is part of the Internet Options settings. This will, however, only block the resource on the one specific PC whereas the Sky Broadband Filter, or a Proxy Server, will block the resource across the whole network.

- **Update firmware:** Of course, not all of these features may be available to you if the router has not been updated. If it still has its factory firmware, a number of these additional features may not have been added to that version of the firmware, so it is a good idea to keep your router up to date by periodically checking for firmware updates.

Be careful with updating the firmware! This is more dangerous than a Windows update and, as with a BIOS upgrade, if the power is lost during the update only part of the new binary image will be stored on the chip, rendering the device unusable.

- **Physical security:** Changes to the router, even its removal and replacement with an

alternative, are only possible if you can get to the router. Protect the router from unauthorized access by implementing a Defense in Depth model: for example, security zones, locked doors, and separate keys to access the device. Keep it in the center of the building where the attacker would have to traverse through several security zones to get to it. Sometimes the quickest way of performing a DOS attack against part of the network is not to attack the hardware with code, but simply to unplug it.



# Exam questions

1. A user receives a pop-up window stating that the PC is infected. She presses the close 'X' button but the PC goes haywire, opening lots of other windows. The disk is thrashing and clearly a virus is at work. How should the user have safely closed the window to avoid triggering the virus?



- Answer:
2. What can be done to protect from a zero-day attack?
    - Answer:
  3. What kind of attack is an ARP poisoning?
    - Answer:
  4. What is a zombie?
    - Answer:
  5. A security guard checks that a member of staff can access a security zone by looking for their name on a duty list. What is this process known as?
    - Answer:
  6. Why is the Principle of Least Privilege more secure than the Principle of Most Privilege?
    - Answer:
  7. What system tool stops a standard user from being able to make significant system changes, including application installations?
    - Answer:
  8. When working with hard drives, what two options do we have controlling how BitLocker encrypts data?
    - Answer:



9. A user reports that they cannot find the Wi-Fi access point within their office location. You know that the access point exists and is working as other users are connected to it. What security action have you implemented here, stopping unauthorized access to the access point?

- Answer:

10. You give old hard drives to a third-party company who specializes in data destruction. What object or document are you expecting to be sent to you once the job is done?

- Answer:



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide.

- **Securing a SOHO Network (13:09):** <http://www.professormesser.com/free-a-plus-training/220-902/securing-a-soho-network/>



# Summary

This chapter is a gentle introduction to concepts covered in the later Security+ course in further detail. We have identified a series of attack types, initially by outlining some basic principles, such as the differences between viruses, worms, Trojans, bots, rootkits, or ransom ware, identifying these as bad for the system in that they affect system instability rather than just being an annoyance. We then considered the Defense in Depth concept and looked at physical security mechanisms you might want to put in place to protect your network further from attack, access by an unauthorized user, or data theft.

From a logical security perspective, we then identified the logical security groups available within Windows. We extended this analogy by considering how we can use security permissions on NTFS volumes and shared folders, and also how these combine together to give an effective permission for the user. We looked at other sign-on principles such as single sign-On; the concept that you only need to sign onto the network once - your session token is used instead to identify you so that you are not prompted for a password if you try to access other protected resources, but uses the token instead.

We then considered best practices concerning passwords and domain accounts, discussing when you enable user accounts, the fact that the guest account should not be used as it presents an auditing problem, but also how accounts can be restricted but forcing the user to change their passwords often, ensuring that the password is strong and not one that has previously been used.

We then extended the concept by looking at mobile-specific devices, looking at remote-locking, gesture control, and other security mechanisms used to lock a phone. I explained that an Apple iPhone, after 10 unsuccessful attempts will reset, so backing up data to the iCloud is quite important. I also described the two paradigms--Bring Your Own Device versus Choose Your Own Device.

I then looked at how data stored on hard drives could be disposed of and the various techniques we could apply to do this, some destroying the hardware and some resetting it. Finally, and most importantly, I detailed the various security hardening techniques you would apply to Wi-Fi access points on your network.





# Software Troubleshooting (902.4)

We may have a great network system, but often things will go wrong, or be misconfigured. One of the key issues is due to hardware age and software updates reaching a point where the hardware is no longer compatible. Equally the application is updated and no longer works on a current OS, or the current OS is no longer supported by the vendor. In all of these cases things can start to go wrong. Let's look at how this tends to happen.





# **902.4.1 Given a scenario, troubleshoot PC operating system problems with appropriate tools**

This is an important chapter in that I am going to try to align some of the troubleshooting fixes you will perform with specific problems that you will encounter. We will start by looking at common problems--what does this look like? How might it manifest? What is the extent of the damage across the network? We will then consider which tools are the most effective in each case.



# Common symptoms

I hate to see these. You know that when you get to the stage when you see a Blue Screen of Death that there is a serious issue, often caused by a recent update which has made the system either partly unreliable or completely unresponsive. These are tools we can use to check these (for example, Reliability Monitor in Windows, assuming that the system still boots up), or may have to resort to an alternative boot system (for example, Safe Mode in Windows), or default to factory settings (for example, Android dead robot screen).



# Proprietary crash screens (BSOD/pinwheel)

A Blue Screen of Death is caused by an execution in memory that has led to one address space that stored a critical part of the OS system to fail because the data has been damaged by an overwrite of data from somewhere else. They are also triggered when the RAM has completely run out of memory, or (on older Windows 95 systems) where an interrupt request triggers two pieces of hardware that are using the same IRQ, which causes a conflict of data. You will get an immediate halt and the system will be completely unresponsive. The blue screen shows the affected area or memory, or an error message explaining that a hardware fault has occurred.

The remedy for this is to power off the PC and reboot it. BSODs are caused where a system change has taken place that was unexpected and led the system to become unstable. Have you installed a new driver recently, or a new, untested application? If this is the case then the BSOD may become a regular occurrence. The fix is to identify a known good time when the system was stable before the change you have made and use system restore to roll back drivers (or replace the driver you know is causing you the problem with another version of it) and software to this point in time.



# Failure to boot

The system has a secondary failsafe set of boot files. This Safe Mode can be used to make repairs to the main system, such as to replace a driver that is stopping the system from booting normally.

If upon booting, after the `POST` test you get a Missing Operating System message that would imply that the boot configuration database is either incorrectly pointing to the wrong partition to find the OS files, or is not being found at all. If this is the case you need to consider booting into the F8 advanced boot menu (if you can, otherwise access it via the installation DVD) and running the `FIXBOOT` command, or `FIXMBR` if you suspect that the Master Boot Record (a table that shows all partitions on a disk) is not readable.

If you have attempted to dual-boot the PC by installing a second OS a new BCD will be created and it is this new one that needs to be read in order to see both OS installations. The new OS needs to be installed in a different partition to the original one.

If you suspect that the Windows files are damaged, once you have gained access to the F8 advanced menu you have the option to run Startup Repair. This interactively tests the BCD and tries to load the OS, alerting you if this was not possible. From the `F8` command prompt you can also rebuild the BCD by using the command `BOOTREC/REBUILDBCD`, which will scan the PC for all OS present and rebuild the BCD with what it finds.

From the F8 menu you also have the options to repair or refresh the PC. Repair will replace system files, but leave user data and settings as they were. Refreshing the PC ignores old settings and replaces everything, pasting over the old Windows structure and replacing the registry with a new one. This should really only be used as a last resort.





# Improper shutdown

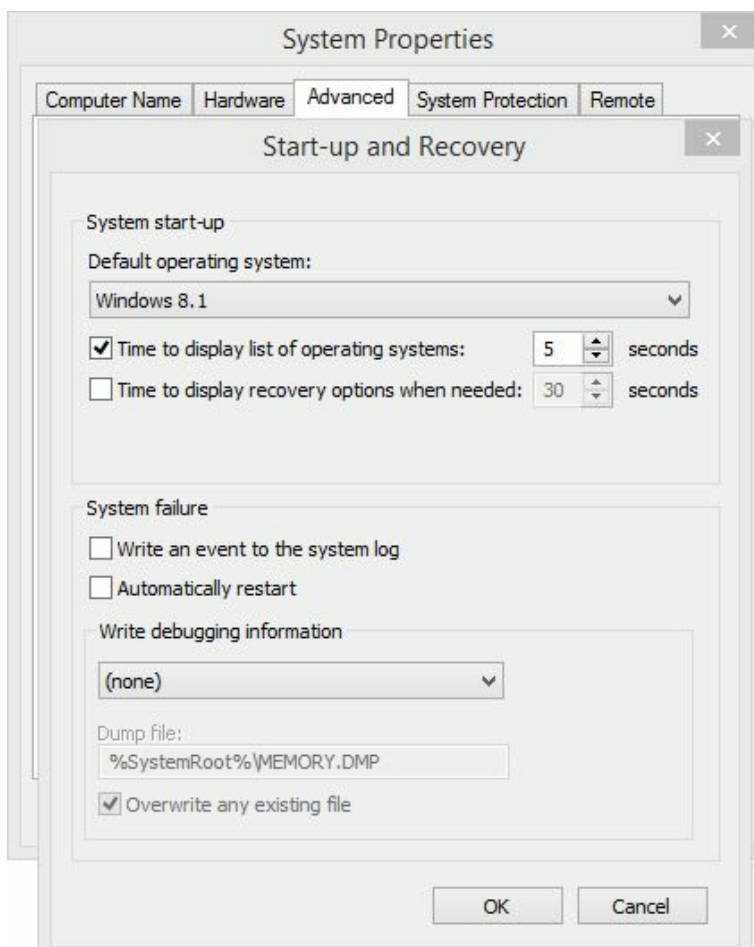
When you ask a PC to shut down it closes down in stages, saving the user profile and any system changes made to the registry. If you power off the PC rather than allowing this shut down to occur as it needs to then changes may not be saved and the user profile could become corrupted. Thankfully, Windows is a pretty resilient system and is able to repair most damage caused during power loss. With Windows XP and earlier systems, however, the potential for damage to the disk structure on the hard disk was there, so you were prompted to scan the hard disk for errors.



# Spontaneous shutdown/restart

If the system restarts all by itself, this implies that it is not stable. This can be caused if the BIOS settings governing the video card memory or processor frequency have been altered. Within Windows, the OS might think that the system is unstable if an application hangs. However, a hanging application might not be such a big deal to the user.

Windows, however, will attempt to recover by restarting if you have given it permission to do so. In the advanced system settings page, on the Start-up and Recovery page there is a section called System failure in which a box is checked to Automatically restart. If you uncheck this, the system will not deliberately restart whenever it encounters what it thinks is a problem.





# Device fails to start/detected

Within device manager, you occasionally will see a black exclamation mark on a yellow background indicating that a device is in a problem state. This is usually due to the fact that an incompatible driver has been assigned to it that is not sending the correct data to communicate with the hardware, so cannot start it. If you are seeing this then it is highly likely that the hardware device affected is not system-critical otherwise you would not be seeing this message at all (the OS would not have started).

Here, the fix would be to check for hardware conflicts and uninstall, and then reinstall the device with the correct drivers.



# Missing DLL message

If you see the message indicating that a DLL file is missing, this can be easily fixed with the system file checker. Run `SFC/SCANNOW` to replace any missing or damaged DLL files.





# Services fails to start

Services are hierarchical. Some services have dependencies, so my first check would be to go into the Services window (`SERVICES.MSC`) and try to manually start the service, then if this did not work check that the services it is dependent on area already started, then retry to start the service.

If the service still does not start, boot into Safe Mode and try to start the service. If it works then it is likely to be a non-Microsoft service or driver that is interfering in the service, stopping it from running.

If you suspect damage to the OS files, as with the earlier fix use system file checker to repair the OS files to the original versions.

There are some specific known errors with some services. Refer to the Microsoft Knowledgebase website for articles covering specific fixes for these (for example, **KB943996** and **KB2839217**).



# Compatibility error

If the program was designed to run on an earlier version of Windows it might not be able to run on the more recent version. By right-clicking the program file and selecting the Compatibility tab you can either run the troubleshooter, which will try to determine what fixes to use, or you can manually set the compatibility fixes you would like to try. If you know that the program worked OK in Windows 7, select the mode and this will use a different set of framework code to trick the program into thinking that it is on a Windows 7 OS. Sometimes the program will not load because security permissions are not allowing it to do so. If you suspect that the program needs to run in the context of the administrator account this can also be enabled here. If the program opens but the size of the window is incorrect you can adjust the color mode and force VGA resolution.

Sadly, some games require video and audio codecs and code frameworks that are no longer used. Without installing these legacy codecs the game would not be able to render.



# Slow system performance

The main reason for slow performance is one application that has priority use of the processor and is taking up so much of the system's resources that other legitimate apps and the OS itself are having to wait. I use a program called BOINC that allows me to engage in Grid Computing, but it is very processor hungry. For BOINC to run its simulations I might set it to have high priority and use 95% of my processor cores. This is fine if I am not using the PC, but when I do need to use it BOINC needs to be throttled back, or paused. I have a setting in BOINC that when the PC is not idle BOINC will automatically pause.

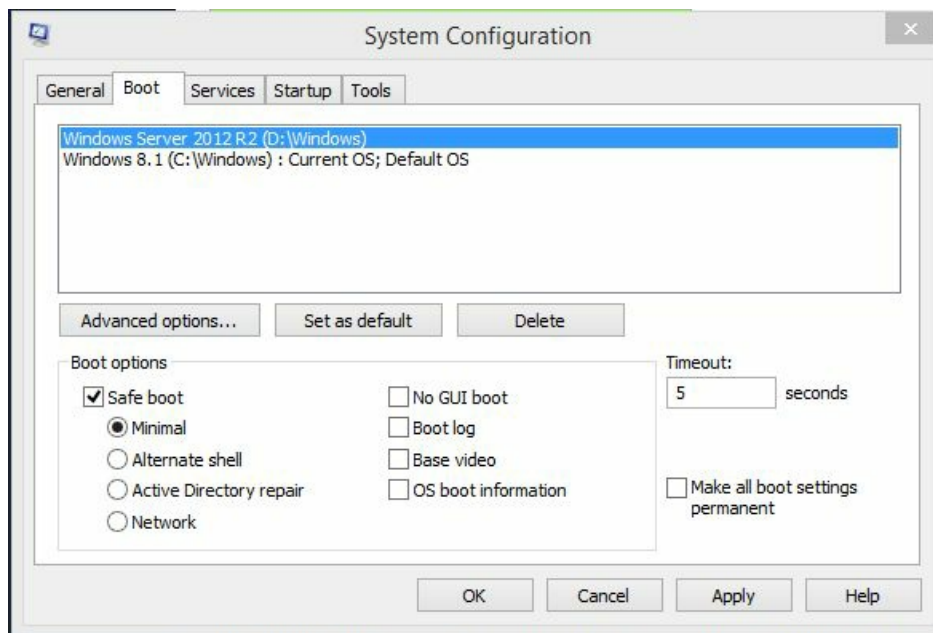
You may notice slower than usual performance when the hard disk is heavily fragmented. This is because it is taking longer than usual to re-piece the files and store them in memory. Naturally, the solution here would be to clean the PC using the internal clean tool, or a third-party application such as Piriform Ccleaner, and then also to defragment the hard drive using either the built-in tool or a third-party application such as Piriform Defraggler.

Later Windows systems such as Windows 10 will automatically defragment and perform disk checks (maintenance mode) on a regular basis, typically once per week but this can be set to require that the user initiates these through Action Center.



# Boots to Safe Mode

One reason why the OS has booted to Safe Mode is because you have asked it to. Within the System Configuration tool, on the Boot tab is an option for Safe boot. If ticked then the system will permanently boot into Safe Mode until you remove the tick.







# File fails to open

There are two possible causes for this:

- You are trying to launch a file via a shortcut, or link on your taskbar, but the file has been moved to a different location. Delete the shortcut, find the file, and if you still need the shortcut remake it and move the shortcut back to your desktop.  
Alternatively, you could just move the actual file back to its original location.
- You are trying to open an `.exe` file. On later systems such as Windows 10 it is common to see that `.exe` have been deliberately blocked. This is a registry setting and can be amended by going to `HKEY_CLASSES_ROOT\exefile\shell\open\command` and setting the default value to `"%1" %*`.



# Missing NTLDR

This is a much more serious problem.

First let's just check that we don't have a non-bootable CD-ROM or DVD-ROM in the DVD-ROM drive and the PC isn't trying to boot from that. Also check that you have not inserted a memory card into the card reader. What is happening here is that the BIOS is telling the system to try to boot from the first boot device in the boot list. If that does not have a list of bootstrap files (for example, a bootable CD-ROM) then it will attempt the next device and so on.

So basically the bootstrap files (for example, NTLDR for Windows XP systems) cannot be found. This could imply that the hard drive being booted from does not contain them, or has been wiped, or your BCD is pointing to the wrong partition, or hard drive.

Windows Vista and later systems use a **BOOTMGR**, so the error message will be slightly different, but the fix will be the same. You should still be able to access the F8 advanced menu, or can do so by booting from the installation media and accessing it that way. Once there, try a Startup Repair to discover the OS partition.



# Missing boot configuration data

This is slightly more worrying as the hard drive partitions themselves cannot be found. This occurs where the BCD cannot be found at all. Again, enter the advanced menu, but this time for the recovery use Command Prompt. Run `BOOTREC/FIXMBR` to find and fix the Master Boot Record, or to overwrite it with a new one. The partitions will again be found. Then, run `BOOTREC/FIXBOOT` to scan for installed OS systems on these partitions, rebuilding the BCD.



# Missing operating system

This normally occurs when the BCD has led the system to a partition that is unformatted, or does not contain any OS files. The obvious fix for this will be to rescan the BCD as previously, but there are other reasons for why you might see this message.

If you have multiple disks in the PC and the first disk contains the OS, but the hard disk cannot be seen in the BIOS because it is either disconnected or simply has died, you will need to check the physical wiring, ensuring that the disk is powered and that the data cable is still connected. If you are using a SCSI or IDE cable ensure that the jumper switch settings are not conflicting with any other disk connected to the system. If necessary, remove the other disks' data cables and add each in turn testing as you go. Hard Drives have a smart error testing facility--you usually get a message a few weeks before the drive will completely fail giving you time to plan to change the disk. If after testing this you are convinced that the disk has died, replace the disk, and rebuild the OS.





# Missing graphical interface

This is less common with Windows, but is a common problem with Linux systems, especially with Ubuntu. If the default graphics driver is not compatible you will need to set the installer to provide a lower resolution that will support it until you are able to completely load all levels of the system. Linux loads in stages:

- System startup (Hardware )
- Boot loader Stage 1 (MBR loading)
- Boot loader Stage 2 (GRUB loader)
- Kernel
- INIT
- User prompt

Also, a number of Linux distros will install, but will boot into the command terminal window. You will need to install a graphic module (for example, GNOME or KDE) with the command `APT-GET INSTALL GNOME` once installed you will need to trigger this from the terminal window to load Gnome.



# Missing GRUB/LILO

**GRand Unified Bootloader (GRUB)** is the Linux boot loader. Older Linux systems used **Linux Loader (LILO)**. If the GRUB is not found the system cannot boot in much the same way as if the BCD is missing in Windows it cannot boot. It is a common problem as the GRUB may have been overwritten by other operating systems if you have tried to dual-boot the system.



# Kernel panic

Linux is a relatively secure system, but is not infallible. Kernel panic is the Linux equivalent to a blue screen of death. It is an unrecoverable error that has made the system become unstable and halts the system. The PC will need to be turned off and restarted, but investigation is required to find the probable cause.



# Graphical Interface fails to load

If the GUI fails to load you will have to resort to removing the hard drive from the PC, adding it to a known good as a second drive, accessing and reading the logs (assuming that you cannot boot into Safe Mode). Every graphics card supports VGA, so you could enter VGA mode to get minimal access to the GUI. If after this the GUI fails to load at all the problem may not be with the card, or its driver, rather with the OS itself in which case you might decide to refresh or reset the PC.

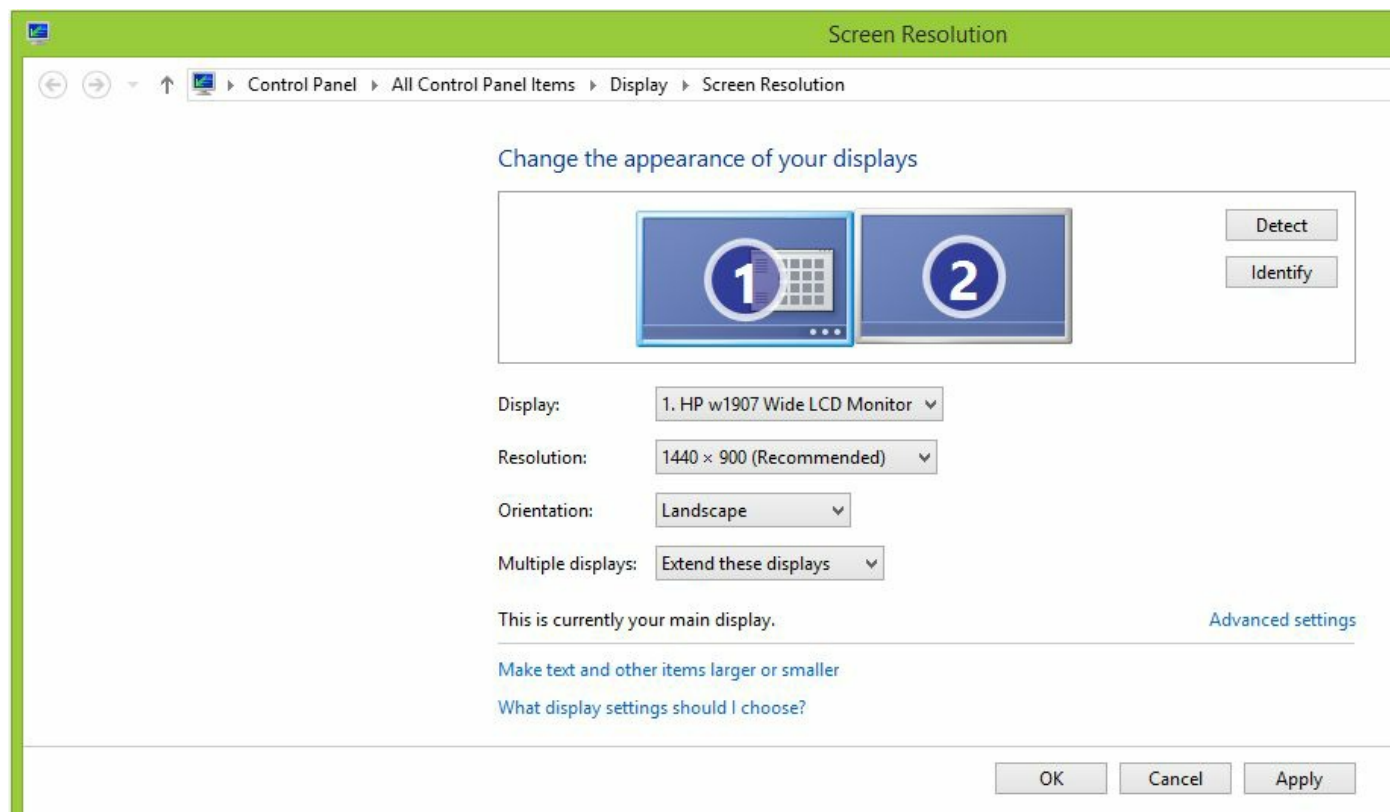




# Multiple monitor misalignment/orientation

By right-clicking on the desktop and selecting Screen Resolution you can change the appearance of each monitor, not only the resolution used, but also the order in which the monitors create the virtual footprint. On my desk my monitors are side-by-side, so I can move my mouse from the left to the right creating one large footprint the size of the space provided to me by the monitors. Last week I connected my laptop to a meeting room HDMI TV that was in front of me, so I added the TV as a second monitor and extended the display, moving the TV (monitor 2) on top of monitor 1. That way my footprint extended upwards, not across.

If the mouse jumps position when I cross from monitor 1 to 2, it is best to check that the monitor's alignment settings within the monitor firmware (on the device itself) match on both monitors. Then, I check that the resolutions are set to the same size.





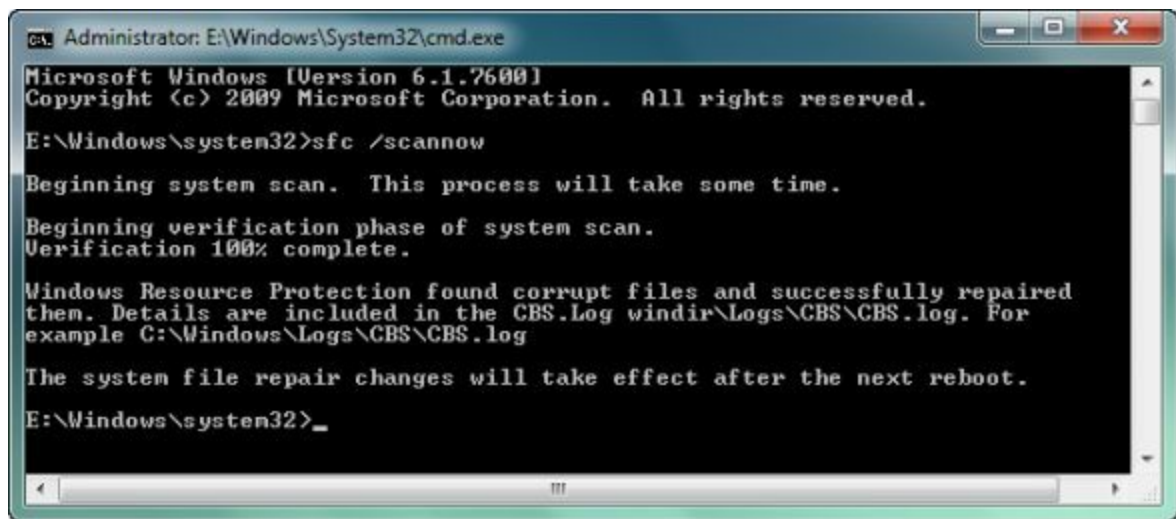
# Tools

There are a number of low-level and OS recovery tools available to us within the OS, as an application or before the machine can start. We will consider some of these here as follows:

- **BIOS/UEFI:** This is the initial firmware installed on the BIOS CMOS chip on the motherboard that instructs the motherboard what low-level devices (for example, disks) are attached to it, the frequency and power settings for the CPU, and other preliminary information needed before the OS can load. As part of this the BIOS also defines if integrated hardware resources are to be used and most significantly the boot order.



- **SFC:** The **System File Checker (SFC)** is an automated tool that tests and replaces damaged Windows system files. It can be used when DLLs do not load, or you suspect that the system is unstable due to missing system files.



```
Administrator: E:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

E:\Windows\system32>sfc /scannow

Beginning system scan. This process will take some time.

Beginning verification phase of system scan.
Verification 100% complete.

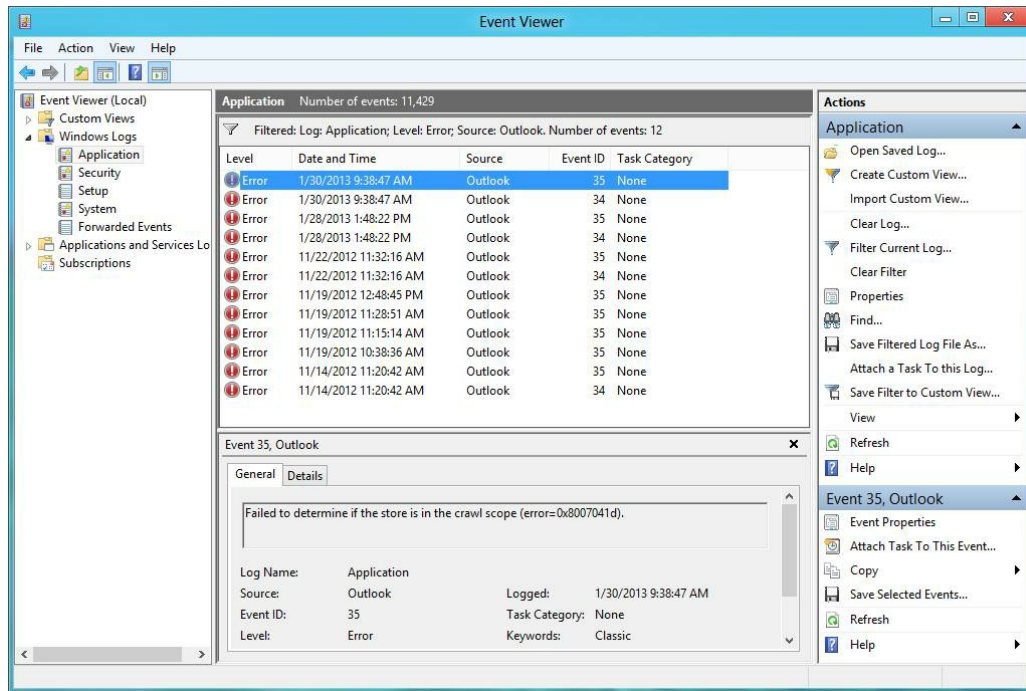
Windows Resource Protection found corrupt files and successfully repaired
them. Details are included in the CBS.Log windir\Logs\CBS\CBS.log. For
example C:\Windows\Logs\CBS\CBS.log

The system file repair changes will take effect after the next reboot.

E:\Windows\system32>
```

- **Logs:** The Event Viewer logs detail all system activity. There are several important logs we use regularly and a good technician will check and fix errors based on information in the logs:
  - **Application:** Any activity related to applications running that do not form part of the OS are listed here
  - **System:** Any system services, drivers, or applications inherent to the OS are located here
  - **Security:** All resource access including logins and shared folder access is located here

The log is a text file that is of a set size, or for an amount of days. When it is full new entries are written at the start of the file, replacing existing data. It is good practice to back up the logs.



- **System Recovery Options:** The Advanced Startup recovery menu provides a number of options for us to repair a damaged system:
  - **Refresh:** Does not overwrite the registry or your user files, but replaces damaged system files with good ones from the installation media.
  - **Reset:** Overwrites the registry. It is a complete rebuild.
  - **System image recovery:** You can use an image file you have previously taken and roll back to this. The advantage of this over Reset is that you have already configured the machine and installed applications onto it, so there is less work to bring the system back to the current point in time.
  - **System restore:** If you know that a recent driver installation (for example) has caused instability you can roll back to a previous checkpoint from here.
- **Repair disks:** You can create a repair disk that contains a tiny bootable command-line interpreter and command tools specific to repairing volumes, the MBR, and BCD. The Windows Recovery Environment is effectively a repair disk. On Windows systems the repair features can also be triggered from the F8 advanced boot options menu, or by selecting the repair option from the installation DVD.
- **Preinstallation environments:** Similar in some ways to Windows RE, the Windows preinstallation environment is actually a file called `BOOT.WIM`. This is a prepared thin bootable image containing a command line interpreter, basic network drivers and graphics support, and little else. You can, however, customize the Win PE image to inject your own drivers and to connect to network resources (mapping a drive letter to a file server). These are used as an intermediary step in deployment and imaging where you are trying to install in image onto a PC that has

a non PXE compliant NIC, or is located outside of the subnet, behind a router that does not support BOOTP protocol traffic. To circumvent the problem you have to assign an IP address to the empty PC first and the Win PE disk can already be preconfigured allowing us to then obtain the image file from our deployment server.



For further documentation on Windows PE read here: [https://technet.microsoft.com/en-gb/library/cc766093\(v=ws.10\).aspx](https://technet.microsoft.com/en-gb/library/cc766093(v=ws.10).aspx)

What does Windows PE look like? Well, when you first install the Windows system, after the first reboot you get a welcome message and the section where you add the license key - that is the same engine as is used for Windows PE.

You can also build your own Windows PE image using the **Automated Installation Kit (AIK)** for Vista and 7 users, or the **Assessment and Deployment Kit (ADK)** for Windows 8 and later users.

- **MSCONFIG:** The system configuration utility is a useful menu to check the boot options, interactively load and test drivers, view background services that are running, and also access 18 other administrative tools.
- **DEFRAG:** The built-in disk defragment utility is used to place files into contiguous order within the volume. If a disk is more than 5% fragmented the level of fragmentation steadily increases making it more time consuming for the system to re-piece files before they can be accessed.
- **REGSRV32:** This command-line tool is used to register a dynamic link library file with the system. These files contain code, data, and resource information and most often drivers are in fact DLL files.



I used to play an interactive adventure game made many years ago to run on Windows 95, but it used a now defunct audio codec. I had to register the DLL before the codec could be used, there was no installer file to do this for me.

- **REGEDIT:** WARNING--Be very careful with the registry editor. Do not delete or change any values unless you are absolutely certain that you know what you are doing. It is too easy to break it and for this reason we deny end-users access to the registry.



Do back up the registry before making significant changes.

That being said, the registry editor is used to add additional configuration changes, or to change existing ones. Please refer to the earlier chapter where we looked at the registry keys (hives) in some depth.

- **Event viewer:** This allows me to search, filter, and read the event logs on the computer. More common on a domain is to send all event logs from every PC to a central folder where management software such as System Center can read them all and aggregate how many machines have which kind of error. Through training System Center to respond to different errors the network can self-heal. System Center uses an Event Collector set--a logging server which acts as a central repository where your event logs are stored for analysis. A self-healing, intelligent network should be your ultimate goal.
- **Safe Mode:** A separate set of loader files are kept in an archive cabinet. These can be used as a second environment, allowing you to test and make key changes to the main loader files and configuration, removing or installing software to overcome issues you are facing.

It is quite obvious that you have entered Safe Mode as the Desktop will be in VGA mode, with a black screen with the words SAFE MODE in each corner. Network and CD-ROM access may be limited whilst you are in Safe Mode.

- **Command prompt:** The command window used to in fact be the MS DOS system, which on earlier systems such as Windows 95 and ME relied heavily on DOS to perform its file operations. Now Windows is DOS independent and relies on its own NT kernel, which is more secure, faster, and stable. The command prompt window is a command-line interface allowing you to run commands not otherwise available within the OS system by using the GUI. Many of the commands have switches extending the capabilities of the command even further. Many commands that make changes to the system are locked out of standard Command Prompt, so you need to run as administrator to allow the command prompt to have full access.

PowerShell is the new replacement of the Command Prompt and in Server 2012 replaces the Command Prompt in the Start Menu jump list. PowerShell accepts some legacy UNIX commands and has equivalents of the DOS commands. You can enter a PowerShell session from the Command Prompt by typing `PowerShell`



and `Exit` to return to the Command Prompt.

- **Uninstall/reinstall/repair:** From the Programs and Features list you can install an application (rather than using the installer MSI file or setup file both located on the installation media). You can also repair a damaged app that is listed by selecting the repair option, which re-pastes the application files into its environment. You can also uninstall the application that deletes the related files and folder structure used by the application, but also registry settings pertaining to the application.

Uninstall processes are often not very good, so over time the registry gets clogged up with superfluous configurations relating to long-gone applications.

**Piriform Cleaner** has a section to clean the registry, removing unused entries.



# Video training

To summarize this section I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Operating System Troubleshooting (14:07):** <http://www.professormesser.com/free-a-plus-training/220-902/operating-system-troubleshooting/>
- **Operating System Troubleshooting Tools (10:01):** <http://www.professormesser.com/free-a-plus-training/220-902/operating-system-troubleshooting-tools-2/>



## **902.4.2 Given a scenario, troubleshoot common PC security issues with appropriate Tools and best practices**

In this section, we are going to detail many of the common issues you will encounter with advice on the best tool to use to remedy the situation.



# Common symptoms

Browsers can receive instructions not only from you but the web server and also other web servers used to draw the different parts to the web page. Some of these may be advertisements or other irritants which may slow down productivity or hamper the users' enjoyment of the page.

- **Pop-ups:** These are far less common now, but still occasionally do happen. More an irritant than anything malicious, some free-hosted websites are funded through displaying adverts. With most of these the advert is built in to the webpage and starts when you scroll down to that section of content. This is the case with PC games, wikis, or online newspapers that will contain a video advert, or other display advert that deliberately obscures the text until you click to remove it. These cannot be resolved because they form part of the webpage itself.

Quite often pop-up adverts appear in a separate browser window designed to appear over the top of the website browser window, obscuring its view. The remedy here is obvious--in Internet Options | Privacy tab click to turn on the pop-up blocker. The pop-up blocker, once turned on has a settings button where you will find an allow list. Some websites legitimately show extra information in a separate browser window, such as a bank would show you if you session has timed out, or have a counter to show how long you have left on a test. Where there is a legitimate use of the pop-up that does not affect your work you can add these sites to the allow list.

- **Browser redirection:** A more serious problem is browser redirection, often caused by a low-level virus changing your browser homepage to another page of their choosing (normally an advertising server). Sometimes it is not obvious that there is a problem--one incident that I had to fix was a user who had set their homepage to Google. The redirection server had a copy of Google's main page, so the user had been duped for some time. There were two giveaways--Google now customizes their main page with special graphics for key dates, also the URL was no longer [www.google.co.uk](http://www.google.co.uk). If I hovered over the Google graphic the inspector at the bottom of the browser showed that if I were to click on here it would take me to an advertising site, not to my intended location.

The quick fix is to go into the Internet Options | General page and change the homepage back to Google. However, I noticed other places within the OS where

the instruction would be rewritten. The second step was to check to see if this was the same with all browsers. If only Google Chrome was affected, then reinstall Chrome.

As a precautionary measure I checked the hosts file located at `C:\Windows\System32\Drivers\` to check for references to an external web server. The only entry that should be there is:

```
| 127.0.0.1 localhost
```

Another check I like to make is to enter the Registry and to navigate to:

HKEY\_LOCAL\_MACHINE | Software | Microsoft | Windows | CurrentVersion | Run

In here you can see if any rogue software is running when you log into your PC, connecting you to an external web server that will re-impose any adware you may have picked up and undo any changes the technician has made to remedy the PC.

Finally, and more obviously, run a malware and anti-virus scan.

- **Security alerts:** Not in themselves dangerous, a security alert is designed to remind the user to run an antivirus scan, and update or to alert you if your antivirus protection or firewall are turned off. On Windows 10, Action Center has an Android look and feel about it with a series of buttons to activate/deactivate certain communication and power features, but also a notification center--the user is alerted with advisory information.

As a rule, always have at least one antivirus program monitoring your system. Always leave your firewall turned on.

- **Slow performance:** This is usually caused by an application working overtime in the background. The question is, what is the program? What is it doing, and did you allow this? Systems do run maintenance tasks at key times, but the technician can set these either in the program itself or if it is set up as a scheduled task, to run at a specific time of the day where its use will not impact on normal operations. Typically these programs may be to defragment or clean the hard drive, to perform a backup, or to run an antivirus/malware scan.

Task Manager is helpful here. You can visually see from the graphs which of the four key hardware components are running hot and from this which program is using most of this resource. Once you have identified the program you can close



it and reschedule it to run at a more convenient time.

- **Internet connectivity issues:** This can be trickier to resolve than you might think and it is best to apply a discipline on how you troubleshoot this. I prefer to use the Command Prompt over the Network Adapter screen, but I will describe Network Adapter first for a Domain-joined computer:
  - In the Network Adapter screen, identify which NIC you are using to communicate with the domain. Against the icon graphic will be a status update. If this says not connected, then the problem is obvious--the Ethernet cable is not plugged in either at your end, at the wall socket, at the patch panel in the IDF, or to the switch in the IDF. You are looking for a physical connection to the switch. Once plugged in you will see an activity light on the back of the physical NIC itself, also on the switch plug, satisfying OSI layer 1.

The status screen will update and hopefully will report the domain name you have joined. If you get a message to say that you are on an unknown network the DNS server could not be contacted, or has not replied back yet. Right-click on the icon, select details, and look at the status information for the NIC:

- **IP address:** This should be in the same order as the default gateway. Find a known good address from a neighboring computer if you need to. For example, my subnet here is 192.168.1.0 with a subnet mask of 255.255.255.0. I know that my nodes therefore are 0.0.0.1 through to 0.0.0.254. My router is my default gateway, listed as 192.168.0.1, so the rest of my network is from 0.0.0.2 upwards (I am using a classful class C address).

If your IP address is assigned by DHCP, you will automatically obtain an IP address in the same subnet as your neighboring devices. If the listed IP address is 169.254.x.x this indicates that you are trying to use DHCP, but the DHCP server cannot be contacted at the moment, so your PC is using an emergency addressing system known as **Automatic Private IP Addressing (APIPA)**. However, all DHCP-enabled computers would experience the same problem and switch over to APIPA, you should still be able to communicate with these, just not access the internet or resources outside of your subnet as APIPA is not routable.

If you feel that your IP address is correct, try to ping a neighboring PC by its IP address. If this is successful there is no problem through the switch, so you can

communicate across the subnet. Try pinging the router with both its internal and external IP addresses. If both of these work there is no issue with the routing table and you can escape the subnet. This implies that the problem is not local.

Try to ping other resources, such as the Domain Controller by its server name. Assuming that your DNS cache is clear, your request will be sent to the DNS server first, the address resolved, and then the PING enacted. This proves that you can access both servers.

Finally, try to PING an external address, such as ping [www.google.com](http://www.google.com). If this works it proves that the external router is connecting to your ISP who is resolving requests.

Yesterday, whilst writing this book, my Sky router lost internet connection. I had to perform this very task. I checked the local network, then my router, and then found I could not PING outside of my network. I went on to the Sky router's management webpage and noticed that the modem was disconnected. This was a problem external to me. Although I restarted the router that would not have fixed the problem as the problem was further down the line, presumably at the exchange. After 10 minutes the problem was resolved.

- **PC/OS lock up:** Thankfully lock-ups are now quite rare due to good power and heat management. Here, we are not discussing BSOD/Pinwheel issues, rather that the machine has stopped working because of hardware settings issues at the BIOS level, or a conflict between two hardware devices (for example, modem and sound card) has caused the system to hang. It can be caused by software-related issues (for example, you are low on memory and have too many programs open), by a virus that has caused the system to become unstable, or by driver-related issues.

Having tried all of these, it is possible that your OS is damaged and needs to be refreshed, which can be done from the F8 advanced options menu.

- **Application crash:** An application stops responding usually because of poor programming (for example, usage of divide by zero). Invalid machine instructions cannot be interpreted by the OS because it hasn't got a clue what the program is talking about. It is possible that the application is trying to write to a memory address it is not allowed to (which has been reserved for system use), so cannot continue. This may be remedied if the application was designed for a previous version of Windows by using Compatibility mode, as different codesets will be

used, tricking the application into thinking that it is on an earlier version of Windows, so code it is trying to execute may make more sense to the earlier version.

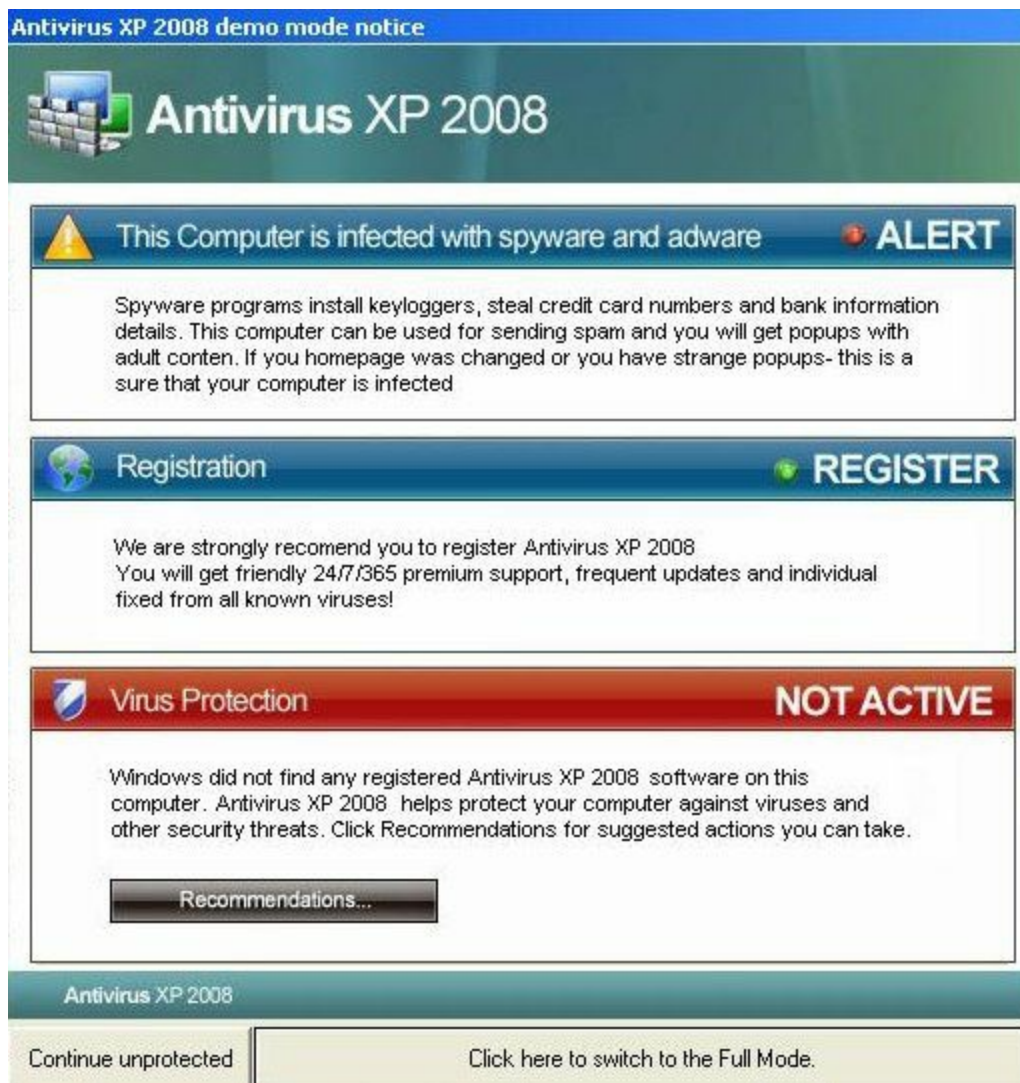
- **OS update failures:** Not all updates are valid for every PC. Core system updates, however, should install and usually only fail if the installation was interrupted in some way, for example, an anti-virus program stopped the installation from running. The first thing to do here will be to visit your PC's update history in the settings cog. Restart the PC and try to run the update again (I temporarily disable my antivirus at this point as I know that the update is trusted). If it again fails to install then Microsoft have produced an Update Troubleshooter (available here: <https://support.microsoft.com/en-us/InstantAnswers/512a5183-ffab-40c5-8a68-021e32467565/windows-update-troubleshooter>). This will interactively test the update and try to fix any errors it encounters.



If all else fails I would advise to revert to a system image and add updates on from this point. If they succeed then you know that it is software you have installed after the image was taken that is interfering with the updates. If updates still fail at this point, I would make a Virtual Machine for testing purposes with a vanilla-build of Windows and add the updates onto this clean copy to verify that the update can in fact install onto the system. If they do install then I would be tempted to build up from this point and then redeploy as a system image onto the host PC.

- **Rogue antivirus:** Some malware tries to fool you into thinking that you have a virus on your PC when actually you have not. This is a social engineering attempt for you to click further on the link, or the application and by so doing trigger other events, such as a malware attack. The ultimate aim is to scam you - you may be convinced that their antivirus software has picked up viruses your known good antivirus software has missed, especially when you click the scan now button and it seemingly finds lots of them! If you unpick the code used at this point you will see that it's not actually performing a scan at all, but showing an animated graphic, pretending to look through your `C:\Windows` folder and identifying a series of known common files. This is enough to trick the unsuspecting or non-IT savvy end user into then buying the software.

Most of these programs do have a Trojan virus fitted, so that they will propagate across the network, fooling more of your colleagues into the same trap. The designers are really just after your credit card details and to confirm that your email address is genuine so that they can perform further scams later on.



Of course, no antivirus software is 100% effective as new viruses are released all of the time. If you still suspect strange activity on the PC I would advise that you revert to a known good clean system image. This is why I like to use System Center as you can roll out a new distribution regularly and at the first sign of difficulty.

- **Spam:** Any unsolicited email is referred to as spam. This is usually unwanted commercial advertising sent out generally to users who appear on an email list. Some disreputable marketing companies purchase lists of active email accounts and send a bulk email to a large number of people.

Your email server is designed to look for key words that might appear in Spam email, but how can you differentiate spam from genuine sales and marketing emails you have asked for? If you have engaged in conversation with the provider then the provider is a genuine person with a real email address.

Because of the fact that you have communicated before, the email will be let through and not treated as spam. Most spam is sent by email servers automatically (bots), so the email address used is not that of a user. This is normally a telltale sign that the email is unsolicited.

The best defense against spam is to never open it. Train the email server to recognize spam by marking the email as spam. This way the characteristics from the email will be recorded and the senders' email address will be blocked.

Remember, responding to spam simply confirms to the web server that your email address is live and can be used to filter their marketing list, which means that you will probably get even more spam!

- **Renamed system files:** Malware tends to do irritating things, but as a general rule most are not harmful to the system, just an irritant. However, malware can rename system files, causing them not to be found, which can destabilize the system. They can also alter security permissions locking Windows out of a folder. In these cases System File Checker will re-add the correct files into place, but not rename the altered ones, nor will it remove the malware. In a situation such as this it is best to go back to a known good image, or refresh the PC.
- **Files disappearing:** If an application disappears, an entry to say that it has exited will appear in the event log. File moves also will be recorded in the event log, if you have asked the system to audit such events (you need to have enabled this beforehand). These are a common symptom illustrating that malware is up to no good. Again, I would be tempted to refresh the PC, clean the user data files separately on a test environment away from the network, and then put them back on afterwards when you have a clean system again.
- **File permission changes/access denied:** Creator Owners are the people that originally made the file/folder and only they can adjust the ACL list. A Creator Owner can remove an administrator from controlling a folder, and also elevate their own privileges even though they may only be a standard user. This presents something of a problem to us. To get around this apply the principle of least privilege and set users to only have Modify rights as their higher most privilege as Full Control gives the user the right to take ownership of a folder for themselves, thereby having full reign of the ACL list.
- **Hijacked email:** One of the ways malware likes to spread is through the use of your email account. If it can access your account it can generate and send a spam email inviting your colleagues to also load malware onto their machines. This is a serious problem because the email was sent by your hacked email account. As far

as spam filters on the email server are concerned the email is legitimate because it was sent by you. End users in terms of digital safety are more likely to trust the email because it was sent by you, and therefore the likelihood of the malware propagation working is much higher. This typically happens when a user's account is compromised. Changing the users password will typically resolve this.

As before, the PC will need to be cleaned, possibly go back to a known good system image. It is not likely that the email server itself is attacked, rather that your Outlook client was compromised.

- **Responses from users regarding email:** Hopefully, the receiving user will contact you back to check that you actually did send this. That should trigger an alert for you mentally that you actually did not send this and that something else is going on.
- **Automated replies from unknown sent email:** Sometimes malware tries to preempt by creating an out of office or automated reply message to say something along the lines of Hey there! Thanks for your email. The software was really good and I think you should try it. Normally due to semantics the email is written not in your style and this should alert someone who knows you well that you actually did not write this (it's certainly not my writing style--it's not florid enough!). Sadly a general email recipient who does not know you may get fooled and worse--the software is impersonating you and you are stating that the software is not going to cause harm. If the person works for a company there is a likelihood that any damage caused on their system will be attributed to you. You may have to argue that you were not the sender and this may be quite hard to do given that the email came from your computer.
- **Invalid certificate (trusted root CA):** I would really worry if I ever saw this. The whole reason for using PKI is to protect the entire network based on a root certificate. The root certificate may be generated by a third party, or made by a local root certificate server. Best practice is that once the root certificate is made, you turn off the PC, remove its hard disk, and keep it in a safe. You then make a new PC and upgrade it to be the subordinate certificate server on the network. Install the original root certificate file onto this PC and then any new certificates generated (service / subordinate certificates) will use hardware information from the certificate server, details in the old root certificate, and a pseudo random number generator. If the root certificate servers were compromised they could not reverse engineer or recreate the original root certificate.

However, they could generate a root certificate of their own and then create a chain of certificates outside of your control given themselves access to your

resources.

But why take the trouble to do all of this? Certificate files provide authentication information to prove who you are. They are also used for encryption and decryption (symmetric), which is fast, secure, and reliable.

It is highly unlikely that the PKI structure of your whole network is affected, however, it is more likely to see this message when connecting to a certificate-protected resource, such as a webmail server only to find that you have been redirected to a dummy webmail server that clearly does not have your certificate installed at its end (a certificate needs to be present at both ends of the connection for encryption to work).





# Tools

We need an array of tools to help to protect our systems before an attack takes place. The first thing to do following an install is to harden the machine with patches and service packs/cumulative updates to ensure that it is not susceptible to zero-day attacks. If possible this should be done by downloading the updates from a known-good clean PC first, saving them onto the network or storage drive such as a pen drive, hardening the new PC offline first before connecting it to the internet.

- **Antivirus software:** This is an application that checks data stored in memory, also on disk whether in transit or at rest for known data signatures found within virus files. It is a matching process and usually very accurate, but is resource-intensive. Most anti-virus applications operate real-time Protection, meaning that it checks data in use at the current moment in time and constantly checks this data.

You will hear terms such as **False Positives** meaning that a legitimate file has a section in its code that matches the data signature for a known virus; however, the code actually has nothing to do with a virus and is not malevolent. As a user you have to train the antivirus program to understand that certain files are safe, or notify an admin to whitelist the file in the central admin console..

- **Anti-malware software:** I tend to use Malwarebytes AntiMalware (<https://www.malwarebytes.com/>), which protects from other threats beyond just viruses. It is a good program to scan for adware, or other annoying code, not just viruses themselves.

Remember that Windows already comes with Defender, which is a pretty good virus protection program and kept up to date automatically by the system.

- **Recovery console:** The f8 advanced menu, also the Windows RE disk, or the recovery section of the installation media all provide access to a recovery console. This allows you access to the system as local administrator to in the command-line perform scans and make low-level changes to the OS. You can alter the boot configuration, partition disks, repair and replace system files, also stop services that may be preventing your system from booting up.
- **Terminal:** In the Linux and macOS world the Terminal window performs the same function. You can alter how applications are configured, adjust configuration files that are used to boot the operating system, and also alter which applications are started/stopped during startup/shutdown.

- **System restore/Snapshot:** We described system restore in detail in an earlier chapter. The system will take snapshots at regular intervals, certainly when significant system changes have occurred, such as the installation of new updates, drivers, or applications. You can also manually create an Restore Point, but first ensure that the OS has sufficient space on the system drive to use to capture these restore points. Each can be several GB in size. With virtual machines, a snapshot is an image of the machine at a specific point in time. You can take a snapshot with the VM PC turned on and if you revert to this snapshot it will continue from the exact moment the snapshot was taken. You are limited to 10 snapshots per VM. Again, each are quite large (several GB in size), so be frugal.

Snapshots are not recommended as a replacement for a backup strategy, although snapshots are a lot more resilient in Server 2016 to a point where they could (but not should) be used as a replacement for backups.

- **Pre-installation environments:** As discussed earlier, the Windows PE is used in a situation where a router is blocking BOOTP traffic, or a NIC does not support PXE booting. Here, a preliminary, tiny platform is loaded allowing access to obtain an IP address, access network shares, and retrieve an image from a deployment server.
- **Event viewer:** The event logs typically are sent as part of an event collector set to a common folder on a file server where system center can read and aggregate them. It will then know which machines need the same fix and can roll-out the same fix, making the job of repairing system problems much easier. As a technician this should be your starting point to determine the cause and extent of a problem and also to gather specific information about the problem before cross-referencing the error code and data with the Microsoft Knowledgebase (<https://technet.microsoft.com/en-gb/ms772425.aspx>) or your own red book (IT Technical database shared by the team).
- **Refresh/restore:** If it looks as though the OS is too far gone for a manual fix, the first option open to you is to restore from a system image. This is because a System Image is unique to the affected PC, contains applications and configuration settings already, and is closer to the current point in time the computer is at (in terms of updates added) than a vanilla-build.

If no image is available, or the system image is too old you may decide to refresh the system by re-pasting the system files onto the Windows substructure. The original registry entries are kept, so no applications need to be reinstalled. The problem with this is that if you are infected by a pernicious virus healing files will only buy you time. The virus may still be active and re-triggers when

you next start up the computer because it is embedded into application code, or re-downloaded from a web server listed in the registry.

The more severe option is to reset. This wipes the registry and basically is a clean installation of the PC. If the virus files are resident in the applications they won't be accessed because they cannot be triggered as the applications are effectively not installed. I personally do not like this option because the infected files are still within the volume. I would sooner completely wipe the drive with a low-level format and start again either with a manual installation, or (preferred) re-image from a known good system image and let system center handle the application installs and updates after this point.

- **MSCONFIG/Safe boot:** We identified a problem where a PC constantly boots into Safe Mode. This can occur if you have forgotten that you have ticked the safe boot option in the System Configuration tool. Unticking this will allow you to get to the main OS upon a reboot.



# Best practice procedure for malware removal

CompTIA prescribes a specific logical order for you to follow, as is detailed here:

1. **Identify malware symptoms:** Note what is happening and the extent of the problem. Try to think about if you have seen this particular kind of action before. Has the antivirus program or firewall been turned off? If so, was this done by the user or automatically by the infecting app?
2. **Quarantine infected system:** Make a note of which machine is infected and remove it from the network as quickly as possible to avoid contamination of other PCs. You probably do not want to switch it off as your Forensic team may want to capture what is going on in RAM and this information will be lost if you do turn it off. Notify a Forensic First Responder of the problem so that they can work with you on the best course of action to take.
3. The Forensic team will want to capture existing data on the infected PC in order to find out what is happening and how this was caused. Your agenda is different - you need the PC to be in working order as soon as possible due to the productivity issue. Best practice here is to satisfy both parties is to provide the end user with another known good PC to use temporarily.
4. **Disable system restore (in Windows):** The problem here is that if you take a restore point, that restore point will contain the virus, so you will end up undoing your good work should you do roll back to this restore point.
5. You could try rolling back to a previous restore point before the virus started to show symptoms, but that is no guarantee that the system is clean. If you have a logic virus it may be scheduled to activate at a set point in time, lying dormant on the system until this point.
6. **Remediate infected systems:** You are now in a position to take action. At this point I tend to move the PC (if able to do so) to a test workbench where it will not interfere with normal operations. The test environment is a sandbox separated from the main network, but still allowing internet access as one of the things you will need to do next is ensure that your antivirus software is up to date:
7. **Update anti-malware software:** If the antivirus scanning software is a free version only you may not have full access to the virus signature database, so a scan may well miss some viruses. Update it to the most recent dictionary first before

performing a full scan. Any files that are quarantined need to be investigated.

8. Scan and removal techniques (safemode, pre-installation environment). If you were to perform a scan in Normal OS mode some of the files in use may interfere with the scan and the scan may not be able to access all areas of the OS. It would be best to update the antivirus software first in Normal OS mode because you have access to the internet. You won't have access to the internet, in fact the rest of the network either in Safe Mode.
9. **Schedule scans and run updates:** Once any affected files have been quarantined or removed and remediation work on these applications has been carried out, update the system to ensure that there are no security vulnerabilities that could be affected should the virus strike again. Set a virus scan to occur at a point in time you know that the PC will be switched on, but not during normal production hours.
10. **Enable System Restore and create a Restore Point (in Windows):** Now that you are certain that the machine is clean, you can return it into the production network and reboot into normal mode. By enabling and taking a restore point you are certain that this point is virus-free.
11. **Educate End-Users:** You will need to debrief the end user assuring them if needed that they are not in any trouble and that their actions have not caused lasting damage. You might want to find out what happened at the time the virus was spotted - what websites were they on? Were they using any non-standard applications? This information is vital to prevent further attacks as you may decide to block access to unmanaged software (for example, Spotify can be a security risk on some networks).



For the exam you will need to memorize the sequence and will get a series of questions looking at a scenario where you have to fix an infected PC. The question will try to describe an activity taking place at one of these stages and you need to identify which stage is being described.



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Troubleshooting Common Security Issues (10:51):** <http://www.professormesser.com/free-a-plus-training/220-902/troubleshooting-common-security-issues-2/>
- **Tools for Security Troubleshooting (7:33):** <http://www.professormesser.com/free-a-plus-training/220-902/tools-for-security-troubleshooting-2/>
- **Best Practices for Malware Removal (5:21):** <http://www.professormesser.com/free-a-plus-training/220-902/best-practices-for-malware-removal-2/>





## **902.4.3 Given a scenario, troubleshoot common mobile OS and application issues with appropriate tools**

In the previous section, we looked at common problems relating to virus attacks on a PC environment. Here we will look at common technical issues faced by mobile users.



# Common symptoms

Focusing on issues faced by mobile devices, especially laptops we are going to take a look at some of the common problems faced and how these may have been caused.

- **Dim display:** This is normally caused because the user has turned the brightness level down within the app settings section. Returning this to mid-way on the slider should resolve the problem. If the user has chosen a power plan to conserve power it is likely that the display will automatically dim when not in use. If the user has enabled power saving, or ultra power saving the display will change to a high contrast theme and the screen will darken to conserve power. Disabling this setting will return the display to normal.
- **Intermittent wireless:** This tends to happen if the user moves out of range of the access point, if there is crosstalk on the channel, or if there is high attenuation. If the signal strength is less than three bars (of five) there is a high likelihood that the packets will be corrupted and fail, leading to a high number of retries, even a loss of communication. At this point the device will automatically retry to handshake with the access point.
- **No wireless connectivity:** If there is no wireless at all, it is likely that the user has disabled wireless, or has triggered Airplane mode. Both of these will stop the phone from transmitting. Simply enable the Wireless button, or disable Airplane mode to restore wireless.
- **No Bluetooth connectivity:** Sometimes a paired device may need to be re-paired, especially if it has not been used for some time. Verify that you are within range, select and forget the device from the Bluetooth list in the phone, and then re-add it as a new device. You will need to re-pair the device.

Sometimes changes on the device itself, not your phone lead to Bluetooth problems. However, there is little that can go wrong with Bluetooth.

- **Cannot broadcast to external monitor:** I tend to use a HDMI connection to an external monitor when broadcasting in my training room, but it is neater to use a wireless solution such as Chromecast. Different phones support different monitor broadcasting software natively so you need to use the correct one. For example, my meeting room TV is a Samsung, so I need the Samsung stream app (Smart View) to be able to send this data from my phone.
- **Touchscreen non-responsive:** This tends to happen for me when I have oil or water on my hands. If you have a black screen this could indicate that either the

device is not powered, or the OS has not booted, in which case you should try to reboot it before attempting to reset the OS. If you hold down the power and home buttons for 10 seconds the device will completely power off before restarting (a hard reset).

- **Apps not loading:** If an app does not load I would question if this is an intermittent fault - was the device stable before the app was loaded? Do I actually need the app at all or could I use a replacement? I would start by rebooting the phone to determine if the current session was unstable, or if the problem is specific to the app. If it is still unstable after a reboot I would uninstall the app, get the phone to a stable state, and find an alternative app.
- **Slow performance:** By checking memory usage you can see if one application is overusing resources, has crashed, and from here can also remove it. On the iPhone, double-tap the Home button to access the memory list. From here slide the application up from the list to remove it. On Android go to Settings and Apps, select the application, and press the Force stop button.
- **Unable to decrypt email:** When checking corporate emails on your phone, even using a webmail browser remember that the connection into the email session needs to be encrypted. You may also need an encryption certificate to be installed on your mobile phone to be able to read encrypted emails. This needs to be supplied by your network manager who may use pretty good privacy, or open standards to send you an encrypted file that when opened will provide you with a certificate file that can then be installed onto the phone.
- **Short battery life:** Most users are unaware of all of the extra features available on their phone and these consume power. For my son, he likes a lightsabre app that turns the torch on as you play with the app. He also uses Instagram, which turns on the camera, but forgets to turn off the camera after he has finished. Both of these hardware components use a large amount of power, so his battery soon wears down. The remedy is to train the end user to conserve power by reducing the apps they use and also to use a power plan to restrict the amount of power used. Also when charging allow the battery to completely run down and then fully recharge it - avoid top up charges as these shorten the duration the battery can hold a charge for.
- **Overheating:** If the processor is constantly running near to full capacity, or you have left the light on, or the display is set to full brightness, then you will generate more heat than normal. The battery will also give off heat during charging. Again, train the owner to use a power plan and be conservative.
- **Frozen system:** These, thankfully are rare, but indicate that the system has crashed and cannot self-recover. You have no option here but to perform a hard reset, but

do check that the system is stable again once it has rebooted.

- **No sound from speakers:** This is a common problem caused either by the user turning the volume to 0% (done by pressing the bottom side volume button), or enabling mute, or plugging in speakers/headphones into the mini jack, or a combination of these.
- **Inaccurate touch screen response:** This is thankfully rare, but there is a screen calibration app you can use to determine where the edges of the screen are and from this the device can work out where you have pressed. You can install an Android calibration APK that will allow you to alter the touch response.
- **System lockout:** Mobile phones have safeguards built into their design to stop other people trying to brute-force attack their way into your phone. We recommend that you never keep sensitive data (for example, family photos) on the device itself, but ensure that a backup to the cloud occurs regularly. With the iOS phone the device will wipe after 10 failed login attempts, if it is enabled to do so. For Android the phone will lock, but not wipe, but if you have associated your phone with your Google account you can use the Google account to unlock the phone. With a Windows Phone, upon locking you may have to re-install Windows onto the phone, or perform a factory reset.



# Tools

For mobile devices we have a variety of areas to look to make changes to, or even to refresh the entire system which are broken into the following possible actions:

- **Hard reset:** This is the process of stopping the system, completely powering down, and then restarting the phone from cold. This is done by holding the power and home buttons down for 10 seconds.
- **Soft reset:** This is the restart option found by pressing the power button and then on the display selecting the restart button within the OS. This gracefully closes the OS and then restarts it, but does not power off devices first.
- **Close running applications:** On Android, if you navigate to Settings | Applications, select the problematic application and then select the force stop button you can close the application that has become unresponsive.
- **Reset to factory default:** For Android users, hold the volume, home, and power buttons to get a hidden boot menu in which you can perform a factory reset, wiping the applications, configuration, user data, and returning the version of Android that originally came with the phone. This is only advised to be done as a last resort.
- **Adjust configurations/settings:** The settings cog provides you access to a large array of configurables allowing you to personalize the phone. There are far too many settings here for me to detail every one. For the context of the exam you need to know that the fix for a particular problem will be to adjust a setting, as opposed to a more drastic solution such as a factory reset.
- **Uninstall/reinstall apps:** If performance is a problem or the phone is difficult to navigate this may be due to a large number of unused apps. Unlike PC programs, but like PC store apps, these games and apps communicate with the store in the background to receive updates, status updates, or to confirm license information. All of this takes up additional transmissions to the cloud, which you may need to manage. For example, I play an RPG simulation game called **Forge of Empires**, which will synchronize game play with an online game server periodically. To see the list of installed apps go to Settings | Applications | Downloads. Find the app you want to delete and press the uninstall button.
- **Force stop:** You can stop an app from consuming resources without having to uninstall it. From the download page as before, select the app in question and press Force Stop.







# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide.

- **Mobile Device App Troubleshooting (9:13):** <http://www.professormesser.com/free-a-plus-training/220-902/mobile-device-app-troubleshooting/>



## **902.4.4 Given a scenario, troubleshoot common mobile OS and application security issues with appropriate tools**

Where the previous section covered mobile apps and typical usage issues, this section will focus on access and security issues when the phone is communicating with a wider network.



# Common symptoms

We often encounter issues with wireless signals often caused by either an interrupted, or weak signal. This section will look at common connectivity issues.

- **Signal drop/weak signal:** We are relying on the signal strength between you and the access point, or radio mast to allow us access to our network. If this signal strength is weak we will experience corrupted and dropped packets, so it will take longer to communicate. If the signal strength is so weak that a signal cannot be sent then the connection (session) is said to have dropped and we will have to reconnect to our access point. This can be set to happen automatically by ticking the auto-reconnect box on the Wi-Fi profile.

You might want to consider running a speed test to determine if you are getting the connection speeds that you are expecting. If not, check the profile first as you may be connecting at a slow speed when both devices are capable of faster speeds. Also check to see what data you are actually sending--is one application hogging the bandwidth? In which case consider stopping the app for now.

- **Power drain:** These are caused when hardware has been activated by an app, or the app is running hot using a lot of resources. You might consider using a power plan and stopping any offending app for the moment.
- **Slow data speeds:** As previously, check the expected throughput you should have by connecting to the access point, or mast. If this is known you can then realize if the overall bandwidth is slow, or data transfer is slow because of other applications sending data in the background without your knowledge that are slowing your transfer.
- **Unintended Wi-Fi connection:** Have you ever encountered an evil twin? This is a rogue access point on the network with the same SSID as a legitimate one, but has a higher power setting. Because of this your mobile device favors this new access point as the signal strength is better. Traffic will be sent on from the Evil Twin to the legitimate access point, but packets will be inspected along the way, passwords recorded, and so on. It is very difficult for an end user to know which of the APs is legitimate, so if you do suspect a rogue AP on the network it is best to report it, where the Network Management team can investigate.

Sometimes the end user performs a Wi-Fi scan and tries to connect to other open APs they are not supposed to in the hope that they can piggy back internet

access. This tends to happen if you are staying in a hotel, so it's best to be careful who is accessing your device (a mobile phone using mobile data set as a hotspot can be connected to by other people).

- **Unintended Bluetooth pairing:** A large number of end users make use of Bluetooth. Wireless microphones, headphones, personal mobile sharing - it's quite common to see (or rather not to see as it is a wireless solution!) Bluetooth in use. It is also possible to connect to other Bluetooth devices you are not supposed to. Bluejacking/Bluesnarfing is the process of connecting to someone else's phone with a view to look through, or taking a copy of photos on their phone, or to send a rude IM message to them. For this reason I advise that you set up Bluetooth pairing, so that anyone attempting to connect to you has to enter a four-digit code.
- **Leaked personal files/data:** Given the fact that we roam in between different cells and access points every day the potential for others to connect to us and take a copy of our data is there. However, the very concept of the Internet of Things requires that your phone sends telemetry about where it is and how it is being used back to the phone provider all of the time. It is therefore good practice to leave mobile data and Wi-Fi switched off until you actually need to use them, otherwise you are exposing your phone to potential risk.
- **Data transmission overlimit:** My son's mobile account has limited data usage. This is because he likes to watch Minecraft parodies and listen to pop music songs from YouTube when on the school bus. That is fine, but he's out of range of our free Wi-Fi, so uses mobile data, which is going to use up his allowance on his account. Within a short amount of time he runs out of mobile data. Do I then allow him to top up by paying for more? No. I have placed a cap on the account to ensure that costs do not spiral.

This is really down to training the end user to be frugal and to be aware of what is going on with their phone. Are apps also using mobile data as well? Do you really want to allow this or could the transfer take place when you are back on Wi-Fi, which will not cost you any money.

- **Unauthorized account access:** It is rare to see unauthorized account access because end users now know to install a swipe lock, fingerprint scan, face scan, or PIN code. However, if the device does not have these security features in place anyone could pick up your mobile, access it, and obtain your friends phone numbers and a whole variety of personal information.
- **One caveat to this is ICE:** The In Case of Emergency list is a small contact list of people the emergency services can phone to notify them of a problem, should you



be unable to do so yourself (for example, you have suffered a car accident and are rendered unconscious. The paramedics could notify a member of your family to meet you at the hospital). The ICE list are people you have approved to be accessed by the Emergency Services. This list can be obtained from the lock screen.

- **Unauthorized root access:** Equally unlikely is root access to the phone. Android and iOS work on the UNIX / Linux model that the administrator only can obtain access to the core system files. The standard user is deliberately separated from this section of the OS. If someone has accessed the root they could cause significant harm to the OS only repairable using a Factory Reset. Not even I know the administrator account for my own mobile phone, so it is likely that such access can only be obtained by hacking the OS using sophisticated crack tools. This is beyond the scope of the A+, however.
- **Unauthorized location tracking:** As mentioned earlier, telemetry is reported back on a regular basis and this is authorized by the user because when you install an app, as part of the installation process you will be notified what data will be sent back to a central server. Any application that did not originally ask for your permission would be deemed as an unauthorized tracker.
- **Unauthorized camera/microphone activation:** A common concern in the past year is the use of viruses to send control signals to mobile phones, tablets, and also laptops to switch on the camera and/or microphone in order to stream information about a user, or to take a photo of the user to use as incriminating evidence.

One interesting example of this is the ShopKick app. This uses GPS to determine that you are actually in the store in question, but also the store emits a high-frequency sound picked up by the microphone as a confirmation code, providing that the user is actually in the store. Another interesting example is 'Pokemon Go', which (although approved) turns on your camera and superimposes a Pokemon animal onto what you are seeing on your display so that you can capture it by throwing a ball at it.

- **High resource utilization:** As discussed previously, check the app list to determine which resources are overusing system resources and make a decision if these need to be stopped.



# Tools

Do how can we protect ourselves from these and what tools are available? This section will list some of the common tools or actions available to you.

- **Anti-malware:** Anti-malware protection scanners are widely available from the Android, Play, and Apple stores. However, I would urge caution to use only known proven brands. The difference in terms of the store is that Apple vets all apps before they are released to the store. This is not the case with the Android marketplace. There are gluts of apps that may look like legitimate scanners, but in fact may do quite the opposite. Also, free versions may perform a basic scan, not checking for all signatures in the virus database and also might not remediate any viruses found, rather instead prompting you to upgrade to the full version.

As part of a Cyber Security audit, if the phone is a company asset it must have antivirus protection installed and working performing a real-time scan. For myself, I use AVG's mobile version that is free and reliable.

- **App scanner:** This is an app that will check to see if other installed apps you have on your mobile device are safe. Such scanners will then initiate a force stop on these applications which allows you a tighter degree of control to your system. I use Piriform CCleaner (mobile version), which is very good at checking applications and conserving resource usage.
- **Factory reset/clean install:** As we discussed earlier, iPhones will reset after 10 (the default is 10) incorrect attempts to log in. A factory reset can be triggered on an Android phone by holding the power, home, and volume key to access the hidden boot menu, then from here you can trigger a factory reset.
- **Uninstall/reinstall apps:** If an app is not working as you would expect one answer is simply to uninstall and then reinstall it. This is often the case if third-party software such as an app scanner has removed key files needed by the app to work correctly.
- **Wi-Fi analyzer:** These are commonly used legitimately by network engineers to determine the geographical reach of each access point, ensuring that they are set to give the best coverage whilst not bleeding the signal out of the external walls. Even the Wi-Fi button, when it performs a scan of the local area for access points is a rudimentary scanner. It reports back on all of the SSIDs found and the type of encryption being used. More complex scanners such as Nessus and NMap have mobile equivalents that will give you data on the local environment. Wardriving

maps such as G-mon can take data that can be superimposed onto a Google Earth map to show what has been found.

- **Force stop:** As discussed previously, you can view the currently running apps and force one that you know you do not need and is using extra resources to stop by using the Force Stop button.
- **Cell tower analyzer:** This is used to get an accurate reading of the speed you are getting when connecting to your local cell tower (mast). Apps such as 'Antenna' will show the connection speed, but in fact status information can be attained through built-in codes that are specific to your telecoms provider.
- **Backup/restore:** Once set up and your Google / Apple account has been associated to the phone backup should be automatic. Your data will copy to the cloud account on a regular basis. To access the backup menu on Android go to Settings | Cloud and Accounts | Samsung Cloud. From here you can see your provider account and set which data components you want to back up, even trigger a manual backup. For Samsung accounts, automatic backup starts after your device has been connected to your Wi-Fi access point for one hour. Backups occur every 24 hours.
- **iTunes/iCloud/Apple Configurator:** iTunes is Apple's music, videos, and pictures library where you can buy or upload your own music library. iCloud is the more generic document storage akin to OneDrive, or Google Drive.

The Apple Configurator is an easier to use version of the iPhone configuration utility. It is capable of performing these tasks:

- Wipe (restore) devices and install a specific iOS release
- Update the installed iOS version
- Assign unique names/identifiers to each device
- Backup and/or restore data from an existing backup
- Create and apply configuration profiles
- Install apps (from the public App Store or created for internal use)
- License paid apps using Apple's Volume Purchase Plan
- Install documents (documents must be associated with an installed app because iOS doesn't offer a user-facing filesystem)
- Assign devices and related configurations to users (users can be populated based on an enterprise directory service such as Microsoft's Active Directory so long as the Mac running Apple Configurator is joined to such a service)
- Organize devices into groups for easier management
- Restrict devices from syncing to other computers
- Assign a organization or user-specific lock screen image

- Create a device check-in/check-out setup that ensures users always have access to their on-device data regardless of whether which device they are assigned (similar to roaming profiles in a Windows business environment where users have the same desktop regardless of which PC they use)
- Enroll devices in a third-party mobile device management (MDM) console for additional capabilities



Details are available at CultOfMac.com: <https://www.cultofmac.com/151560/apple-configurator-perfect-for-schools-and-small-business-but-too-limited-for-many-big-companies/>

- **Google Sync:** This is a synchronization tool allowing users to connect to their Microsoft Exchange server via Exchange ActiveSync through which they can synchronize their email, contacts list, calendar, and tasks with their mobile device.



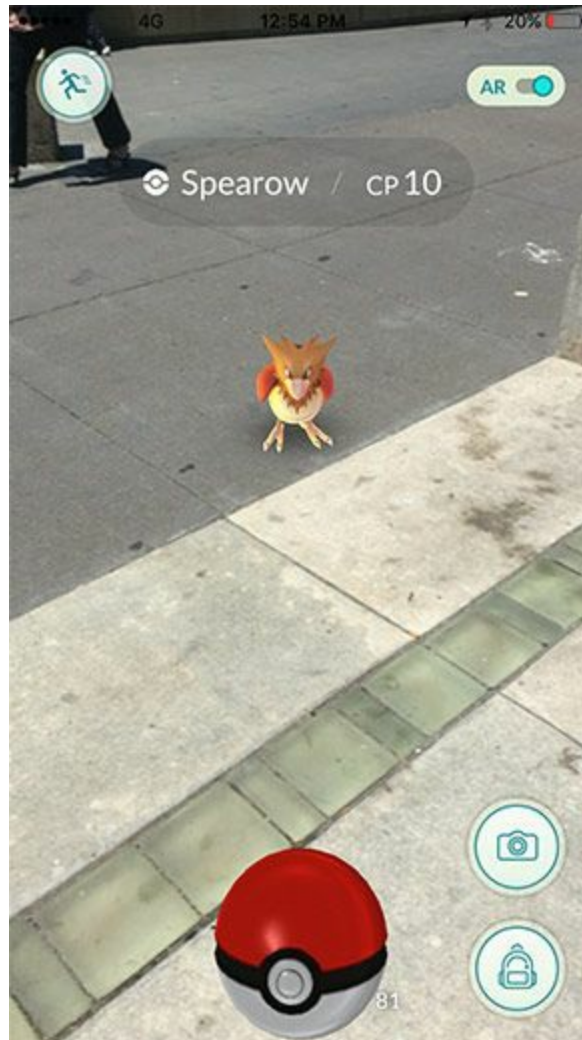
Full details are available here: <https://support.google.com/a/answer/135937?hl=en>

- **OneDrive:** Originally called **SkyDrive**, this is Microsoft's document storage implementation. There are two OneDrives--one is for personal use and provided to home users for personal storage, but **OneDrive for Business** can be linked to a corporate Office 365 environment as well as SharePoint Online so that employees can work with documents whether they are in or out of the office.



# Exam questions

1. You believe that your mobile phone has been stolen. Before you wipe it you would like to try to locate it one last time. The device has been registered with your Google account. How do I do this?
  - Answer:
2. A child user reports that their mobile phone, which is still relatively new cannot hold a charge for any period of time. You notice that they use some games including a Star Wars lightsaber app and Pokemon Go are running in the background. What effect will this have on the power consumption of the phone?



- Answer:

3. A user is using a mail app to view their company email messages. Why would an end user not be able to decrypt their corporate email?
  - Answer:
4. I am on the train. Someone nearby complains that they are getting the wrong music. It transpires that they are listening to a music track I have just tried to play myself and stream to my headphones. What is the likely cause of the problem?
  - Answer:
5. How do I get to the factory boot menu on an Android phone?
  - Answer:
6. How do I perform a hard reset on an iPhone?
  - Answer:
7. A user reports that they are getting general emails advertising services they don't want or need. None of these emails address the user specifically. She explains that they are in a separate folder called 'Junk', in her mail program. She wants to know if she should be concerned by this.
  - Answer:
8. The company CEO reports that they have received an email targeted at them asking for personal information. The sender knew something about the person as they mentioned her favorite football team and information about where the town she lives in. What type of attack is this?
  - Answer:
9. You dual-boot a PC that originally had Linux Red Hat Desktop installed. You install Windows 8 and place the Windows folder in a second partition, but have had to add the partition manually before installing. Once installed, the Boot Manager loader shows both systems. Windows loads fine, but you get an error message when trying to load Linux - "MISSING GRUB". What is the likely cause of the problem?
  - Answer:
10. Name two requirements for using Bitlocker.
  - Answer:





# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide.

- **Mobile Device Security Troubleshooting (5:45):** <http://www.professormesser.com/free-a-plus-training/220-902/mobile-device-security-troubleshooting/>



# Summary

This troubleshooting chapter underpins the entire A+ as there you will be trying to find out what has gone wrong. CompTIA recommends a seven-step process and will be making sure that you know the order to follow here. In the past a number of technicians would try the fix first, but end up either wasting time, or not fixing the problem at all, or making the situation worse. By taking this logical approach and using deducting reasoning, also by sharing fix information with your team and developing a Red Book Knowledgebase you will be able to quickly fix problems that are re-occurring whilst also sharing with the team how to fix newly-encountered problems.

Here, we have looked at a variety of symptoms and contextualized them by stating where you would expect to see this problem occurring, or its trigger. We will also identify some of the tools you may need to use to identify and to remedy the fault.

We then look at mobile devices, looking at problems common to these, and then widening the problem from application-specific to network access or security issues.



# Operational Procedures (902.5)

Ok, so we have focused quite heavily on the technical aspect of the CompTIA A+. If you intend to get and hold a job in the industry there are a few soft skills also required of you. This chapter will cover safety, keeping not only yourself but also the equipment safe as well as others. You will consider environmental safety aspects and policies, then look at broader information security policies used to ensure organisational safety. You will consider Safeguarding (keeping yourself beyond suspicion or reproach) and professionalism, for example meeting targets and ensuring that you meet your department's contractual obligations whilst working within a team.



## 902.5.1 Given a scenario, use appropriate safety procedures

This final chapter is in many ways the most important as I would like you to stay safe and well. Working with electrical equipment is not without some degree of danger, so I would ask that you think about your own personal safety and the safety of others.

Years ago I was supervising an A+ class and two students were playing around. One had switched the power input dip switch on the back of the Power Supply Unit on his friend's PC to US 110 V, rather than the UK 230 V setting. As a result, when his friend plugged in the mains cable a massive surge sent through the PSU blowing the capacitors inside. We heard a loud 'pop' and acrid smoke began to escape from the PSU vents. The young man instinctively threw himself backwards against a table. I ran over to the area, made it safe, and checked that he was not being electrocuted. Dropping the mains cable and jumping out of the way was definitely the best thing to have happened.

As a result he was in shock and was treated for shock by a first aider. I radioed in the incident immediately and filled out a health and safety report. I asked a colleague to cover for me as I made the area safe and alerted everyone who needed to know that there had been a near miss. I spoke with my Head of School and Divisional Director. Later on I was commended by the fact that I had done the right thing, followed procedures, and that the incident was not any worse.

A few years after this I was teaching an A+ course at another academy. One of my neighboring teachers was delivering a class where they were using compressed air (from an aerosol can) to clean a dirty PC. He showed his class a physics experiment-- how the CO<sub>2</sub> from the can could lower the temperature of water to form ice. He sprayed some CO<sub>2</sub> into a plastic cup with some water in the bottom. The water froze.

A few minutes later, I had a knock on the door of my classroom. It was the teacher from the classroom opposite looking obviously intoxicated. He could hardly stand, was giggling, and certainly not his normal self. I opened the windows, got my students to look after him, and called for a Team Leader to help. This could have been more serious than it looks. I then went over to his classroom, made the area safe, and moved the class onto a new activity not involving the air cans, taking these away.

Why was he drunk? He showed the experiment involving the water, but did not think



through the consequences. The aerosol can also releases solvents such as denatured alcohol, butane, and propane, which when inhaled would go straight to the brain, starving the brain of oxygen. I asked a first aider to look after him. He was OK and back to normal within 20 minutes or so, but had quite a headache for the rest of the day!

Why am I sharing this with you? This chapter focuses not only on personal safety as well as equipment safety, but also professionalism. How do you handle yourself in a difficult or unusual situation? Hopefully this chapter will not only keep you alive, but also keep you in your job.



# Equipment grounding

When working on electrical equipment such as a PC the best course of action to take is to remove the power from the device, including any batteries before you commence work (the BIOS lithium battery can stay in place as it holds a very low-level charge and is more trouble than it's worth removing it if the BIOS resets!).

The correct environment would be a clean, well-lit room with a workbench. There should be sufficient room around you to dismantle the equipment and keep note of which parts go where. Where possible and if you are unsure draw a diagram of the insides, or take a photo with your mobile phone. Label any parts you are unsure of and also which wires go where. This is very important when working with MOLEX and IDE data cables to ensure that the same sockets are used when you put the system back together.

You should be using an anti-static grounding mat. The mat has an earth wire leading to a grounding plug, ensuring that the chassis, which is in touch with the mat is at the same voltage as the mat, namely is set to Earth. I also attach a crocodile clip wire from an eyelet on the mat to the chassis, confirming that we have Earth. Next attach an earthing wrist strap to the hand you tend not to use (I am left handed so will hold the chassis with my right-hand, so tend to strap my right wrist). This ensures that you are also earthed.





# Proper component handling and storage

Components are delicate and circuitry can be damaged by as little as 20V (an amount you can hardly feel if the current is tiny). Worse still, you will not visibly notice any damage until the PC is rebuilt where after several weeks you may notice RAM errors occurring. Circuitry is delicate and susceptible to electric shock. For this reason we isolate it from its environment by placing it into an antistatic bag. This ensures that external electrical forces cannot penetrate the bag and harm the component.



# Toxic waste handling

Many components used to make IT systems use heavy metals, acids and other material which are hazardous, but also components such as plastic casings which are not biodegradable. Here we will look at some of the key elements to consider when thinking about toxicity:

- **Batteries:** Many batteries contain heavy metals such as Lithium, which cannot be disposed of in the normal garbage waste as it would poison the environment. Recycling centers will have battery recycling schemes where batteries can be collected and disposed of safely.
- **Toner/Air filter mask:** Print toner is a 2B carcinogen. It is a mixture of dyes, wax, and ionized carbon. The ionized carbon can be an irritant if breathed in. For this reason I recommend using a breathing mask when working with toner cartridge replacements. Photocopiers and laser printers also emit Carbon Monoxide and so they should only be used in ventilated areas.
- **CRT:** Cathode Ray Tube monitors also contain heavy metals, lead, and potassium. As with batteries recycling schemes are available at landfills and recycling centers where the unit is crushed, broken down into components, and these components are dealt with separately.





# Personal safety

Here, we are going to focus on your health and well-being. Electrical safety is of course important to ensure that you are not injured but also to protect sensitive components such as RAM chips. Many IT components are bulky and heavy, especially when still boxed and so manual handling techniques are an important consideration.

- **Disconnect power before repairing PC:** I admit that I at times and in a hurry have not followed best practices--I have removed the inspection cover and ripped a hard drive out of a PC case before now, but it is an extremely dangerous thing to do. Best practice would be to use an anti-static mat and workbench, disconnecting the power to avoid damage to the components and to yourself. Remember that capacitors hold a charge for a long time even after the device is disconnected from the power, so the potential for shock is still present.
- **Remove jewellery:** An electrostatic shock typically occurs because of jewellery such as a metal watch, wedding ring, or bangle hanging into the circuitry, completing a circuit, and causing a short. Electricity always finds the shortest possible route and as you may be using a grounding kit you are earthed, so touching you will have the same effect as if the electricity spark had traveled from the circuit component to the chassis. It's just more painful when the jolt goes through you. As skin is less conductive than metal, jewellery would make a perfect entry point for the spark.
- **Lifting techniques/Weight limitations:** As a staff member in a company of more than five people based in the UK, Health and Safety regulations dictate that you take a fire awareness, manual handling, and safety assessment course plus exam every year. The Manual Handling course lists the following tips:
  - **Plan:** Assess the risks. Figure out the best place to park the van. Know the type of environment you're entering in to. Have all the manual handling aids at hand. Know your exact drop off.
  - **Load:** Store heavy objects at waist level. Balance the load. Make sure the box or vessel is as solid as possible so it doesn't fall apart. If it's too heavy, empty things out and get them on a second run.
  - **Equip:** Utilize manual lifting aids and ladders. Use protective gear such as gloves, safety boots, and outerwear. Rack out the delivery vehicle for safe handling.
  - **Train:** Adopt a good posture. Lift with the legs, not the back. Never twist the spine--turn by shuffling the feet instead. Bear the load in close to your body. Avoid prolonged lifting above shoulder height.

- **Move:** Clear the path ahead. Open the doors, clear obstructions, and make sure you can see where your feet will be, especially when going down stairs.
- **Know the limits:** Be clear on the weights involved by labeling parcels. Stop work when tired or fatigued as this is the time you'll get hurt. Deliberate. Putting your back out is not worth it to save eight seconds.



Courtesy of Michael Brennan, Avenue House Health & Safety Solutions  
available at: <https://www.transpoco.com/blog/2013/12/16/6-tips-better-manual-handling/>



# Electrical fire safety

The following are tips from the Cheshire Fire and Rescue Service covering Electrical Fire Safety:

- **Don't overload plug sockets:** An extension lead or adapter will have a limit to how many amps it can take so, to help reduce the risk of fire, be careful not to overload them. Use the calculator tool (<http://www.cheshirefire.gov.uk/public-safety/campaigns/awareness-campaigns/electrical-fire-safety-week>) to assess whether or not you are overloading an adapter.
- **Regularly check for frayed or worn cables and wires:** Check to see if the cable is fastened securely to the plug and check the socket for scorch marks. You should always carry out these checks before you plug an appliance in.
- **Unplug appliances when not in use:** This helps to reduce the risk of fire. Unplug appliances when you go to bed or when you go out unless they are designed to be left on, like freezers.
- **Keep electrical appliances clean and in good working order:** Look out for fuses that blow, circuit-breakers that trip for no obvious reason, and flickering lights to prevent them triggering a fire.
- **Check for British or European safety mark:** Make sure an appliance has a British or European safety mark when you buy it.
- **Always check that you use the right fuse to prevent overloading:** When you're fitting or replacing a fuse, it's important to use the right fuse for the appliance to make sure the cable doesn't overheat and that the appliance is protected in the event of a fault.
- **Get Out, Stay Out, Call 999:** Never use water on an electrical fire and don't take any risks with your safety. Pull the plug out or switch the power off if it is safe to do so. Get out, stay out, and call 999.

Which fire extinguisher do I use with electrical equipment? The short answer is not a water extinguisher! In the UK, every extinguisher is painted red to denote that it is a piece of emergency apparatus, but has a colored label signifying the substance inside. A BLACK label (Carbon Dioxide) is best for use on electrical fires such as servers and PCs, although you are releasing extra CO<sub>2</sub> into the room, so if the room where the fire is located is small, such as a server room, you should evacuate it first.



You can find a detailed breakdown of each extinguisher (there are four main types) at the FireSafe website: <http://www.firesafe.org.uk/types-use-and-colours->



of-portable-fire-extinguishers/



# Cable management

When assembling a PC it is good practice to use a wiring loom, or cable ties to measure the exact lengths needed rather than leaving wires dangling around within the chassis, as wires may snag on the internal fans and over time chip away the plastic casing, or be cut by the fan blades. More importantly a mass of wires will reduce airflow within the case, leading to poor air pressure and resulting in a heat buildup within the chassis. This in turn could damage components and cause the PC to reset if it were to overheat.

Within an IDS/Server room cable management is essential. Each wall socket should be labeled and correspond to positions on your patch panel. From the patch panel you want to run a patch cable to the switch ports keeping these in order. Labeling the ends of the cables is good practice to make it easier to find the one you are looking for. If you do find that you cannot find the other end of a cable as it is buried in a spaghetti of wires, consider using a Fox and Hound toner probe.







# Safety goggles

When working with any material where shards may fly off, or where a strong light may be emitted, I would advise that you wear personal safety goggles. If you are welding or drilling the chassis the potential for danger is present. Not only should you wear safety goggles, but also tinted glasses to avoid bright light from the weld to blind you temporarily. Equally, if you take apart a DVD-ROM drive there is a laser inside that could potentially send a beam of light to your eye.



# Compliance with local government regulations /Protection from airborne particles

In relation to IT equipment, this involves the correct handling and storage of data. This also covers the use and storage of combustibles. You also need to keep a paper trail on all dangerous chemicals you may be using along with a 'certificate of destruction' where paper or electronic data has been sent to a third party for destruction.

When you buy chemicals such as toner you will notice a **Materials Safety Data Sheet (MSDS)** enclosed in the box. The manufacturer may also have a returns policy so that you return the carcass back to them in a free post box for them to dispose of and by so doing give you a discount on future orders. An MSDS lists the chemicals used to make up the substance. It reports who made the item, who to contact if you have any Health and Safety questions, and where to return it to.

An example Materials Safety Data Sheet sheet is here:



## SAFETY DATA SHEET

### 1. Identification

<b>Product identifier</b>	HP LaserJet 92274A Print Cartridge
<b>Other means of identification</b>	Not available.
<b>Recommended use</b>	This product is a toner preparation that is used in HP LaserJet 4L/4ML/4P/4MP series printers.
<b>Recommended restrictions</b>	None known.
<b>Company identification</b>	HP Inc. 1501 Page Mill Road Palo Alto, CA 94304-1112 United States Telephone 650-857-5020  HP Inc. health effects line (Toll-free within the US) 1-800-457-4209 (Direct) 1-760-710-0048 HP Inc. Customer Care Line (Toll-free within the US) 1-800-474-6836 (Direct) 1-208-323-2551 Email: hpcustomer.inquiries@hp.com

### 2. Hazard(s) identification

<b>Physical hazards</b>	Not classified.
<b>Health hazards</b>	Not classified.
<b>Environmental hazards</b>	Not classified.
<b>OSHA defined hazards</b>	Not classified.
<b>Label elements</b>	
<b>Hazard symbol</b>	None.
<b>Signal word</b>	None.
<b>Hazard statement</b>	Not available.
<b>Precautionary statement</b>	
<b>Prevention</b>	Not available.
<b>Response</b>	Not available.
<b>Storage</b>	Not available.
<b>Disposal</b>	Not available.
<b>Hazard(s) not otherwise classified (HNOC)</b>	None of the other ingredients in this preparation are classified as carcinogens according to ACGIH, EU, IARC, MAK, NTP or OSHA.
<b>Supplemental information</b>	This product is not classified as hazardous according to OSHA CFR 1910.1200 (HazCom 2012).

### 3. Composition/information on ingredients

Mixtures			
Chemical name	Common name and synonyms	CAS number	%
Iron oxide	Iron oxide	1317-61-9	<55
Styrene acrylate copolymer		Trade Secret	<55

### 4. First-aid measures

<b>Inhalation</b>	Move person to fresh air immediately. If symptoms persist, get medical attention.
<b>Skin contact</b>	Wash affected areas thoroughly with mild soap and water. Get medical attention if irritation develops or persists.
<b>Eye contact</b>	Do not rub eyes. Immediately flush with large amounts of clean, warm water (low pressure) for at least 15 minutes or until particles are removed. If irritation persists, consult a physician.

Image source: [http://h22235.www2.hp.com/hpinfo/globalcitizenship/environment/productdata/Countries/us/lj\\_92274a\\_us\\_eng\\_v18.pdf](http://h22235.www2.hp.com/hpinfo/globalcitizenship/environment/productdata/Countries/us/lj_92274a_us_eng_v18.pdf).



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Managing Electrostatic Discharge (3:16):** <http://www.professormesser.com/free-a-plus-training/220-902/managing-electrostatic-discharge-2/>
- **Computer Safety Procedures (5:04):** <http://www.professormesser.com/free-a-plus-training/220-902/computer-safety-procedures-2/>



## **902.5.2 Given a scenario with potential environmental impacts, apply the appropriate controls**

Keeping with the MSDS which is an excellent resource detailing the environmental impacts which may affect the storage of components, we are going to widen the analogy to cover different wider environmental changes which may affect your systems. For example a power outage could cause servers to shut down and data to be lost.





# **MSDS documentation for handling and disposal - including Temperature, humidity level awareness, and proper ventilation**

So now that we've introduced the MSDS, how and where would we use it? Well, a technician should know to check the toner (in the case of the preceding example) is or is not the same as the one that has just ran out. To protect their own safety this sheet will detail any precautionary measures they may need to take (such as wearing a breathing mask). The First Aider and Health and Safety Manager for the site needs to know the first-aid measures to take and may need to train their staff to take additional action.

There may be certain temperatures you have to keep the material at. If it is stored at a higher temperature the substance may break down, or become volatile.

Medical staff may need to know information about the particulates in case the substance is ingested, or a person is otherwise exposed to it.

Disposal considerations are provided in the MSDS detailing how the unit should be disposed of and if further measures need to be taken other than local government compliance.

As an example of an MSDS please visit HP's environment section of their website where you can download MSDS sheets for your country <http://www8.hp.com/uk/en/hp-information/environment/msds-specs.html>.



# Power surges, brownouts, and blackouts

Power is not a stable commodity. It relies on the supplying substation to provide a constant stream at the same level, but power entering a building is often dirty. By this we mean that the signal fluctuates, with occasional spikes and dips.

PSUs are very good at removing most of the spikes, performing line conditioning as the power is channeled through a series of capacitors and resistors first to channel the voltage into a stable pattern. With PSUs we then perform a step down and translation from alternating current to direct current to run the internal components are a greatly reduced voltage (for example, 12 V DC).

You can purchase separate line conditioners that smooth out dirty voltage, but most high-end extension cables can perform line conditioning.



Do not mistake a line conditioner with a surge suppressor (also known as a **surge protector**). Where the conditioner levels the power, the surge protector is an extra plug you add in between the socket and the device plug, which cuts the power to the device if there is a surge.



A power surge is a sustained excess of power, far more than components can handle. This may lead to safety fuses, such as a plug fuse or a trip switch to trip out, cutting power to that section of the ring main. This has the same effect for the PC as if somebody had turned it off at the mains. The system will not have gracefully shut down so work will invariably be lost, but the system can recover.

At this point it is worth mentioning why we have fuses in our circuit. A fuse is a strand of wire designed to be the weakest point in a circuit. If the power were to build up it would be better that the fuse burned out and broke than any other more valuable component on the circuit. Fuses only cost a few pence to replace, where hardware components are very costly:

- A **brownout** is a dip in power enough so that the PC cannot maintain a fully working system. If we are connected to a laptop and the laptop has both a battery present and is also mains powered, although we are purportedly using the mains, the battery is being constantly topped up. If that feed stops, or reduces to a point where the supply cannot keep the system going the laptop will automatically switch over to using the battery reserve. With PCs, it will try to gracefully shut down if it can. Brownouts are therefore localized dips in power affecting a small area.
- A **blackout** as the name suggests is a much wider and more sustained total loss of power. Here, you would need to resort to using backup energies. In the case of a server an **Uninterruptible Power Supply (UPS box)** is a battery box that is constantly being recharged. It has a USB tether to the OS so that the OS knows how much charge the battery has. If the mains power is cut, an alarm will sound. You can trigger a close down to happen automatically, or may want to do this manually, but the UPS box buys you time (typically around 20 minutes, but this depends on the power usage of the server) allowing you to shut down the server gracefully and

not lose any work.

If the blackout is longer-term you may want to consider hiring a generator. Here you will need to switch from the normal mains to a separate feed from the generator for the amount of time the mains supply is unavailable.



# Dust and debris

As we restore PC components you will notice a buildup of dust and debris within the chassis. It is best that you wear a mask and work in a well ventilated room, or outside if it is safe to do so (and not raining). By using a lint-free cloth and foam Q-tips you can gently rub away the buildup of grime.

To help to free sections of dirt you can use either a can of compressed air with a straw to get into the hard-to reach places, or a PC vacuum. These are special vacuum devices that do not emit electrostatic discharge and are safe to use around electrical equipment.



Q-tip and air can





# Compliance to local government regulations

When replacing network cables in a building you need to ensure that you are using like-for-like. Adopt the same TIA standard used as the original cable was. Use Plenum (fire retardant) cable within the Plenum space within the building and once the cable is in-situ, have it certified so that the building insurers know that the cable is to a professional standard and meets compliance regulations.

Remember that there are restrictions on how your components are disposed - they cannot go into the landfill. Please check your local regulations to ensure that you are compliant.



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide.

- **Managing Your Computing Environment (6:24):** <http://www.professormesser.com/free-a-plus-training/220-902/managing-your-computing-environment-2/>



## **902.5.3 Summarize the process of addressing prohibited content/activity, and explain privacy, licensing, and policy concepts**

A number of times in this book I have referred to the concept of Incident Response and mentioned that there are two agendas here - you, as a technician want to fix the fault and contain the problem. A Forensic team has to also look at the legality of the situation - where did the breach come from? Who was responsible? Are there any clues to help us to learn who caused the incident? It's not always obvious and existing data in the RAM may be crucial as will the current image of the hard drive. Let us look at some of the concepts from a Forensic perspective.



# Incident response

The first responder is not the first person to identify the incident, but the first Forensic responder to capture the data at the scene of the incident. This will involve working with the IT technical team to make the area safe, to contain the problem without losing data, but also interviewing witnesses to determine a timeline of actions and general time frame leading up to the incident.

The first level responder captures additional event data and performs preliminary analysis. The first responder determines critical of the event. They may in fact be a first-line support technician.

The idea is to assemble the correct individuals to assess the incident, and then to make decisions on the best course of action to take to get to the best resolution of the incident.

This may, to an IT technician just sound like management speak, and to me when I first started out in Cyber Security it did, but think about it: How many times do you get the chance to witness an incident as it happens up close and personal and to learn from it so that if it were to ever happen again you would be better informed what to do and what not to do? I'm reminded of the sinking of the RMS Titanic. The investigation after the incident led to conclusions that some courses of action taken were wrong and that further lives could have been saved. As a result of this catastrophe, life jackets, lifeboats, and warning equipment became standard. Think about the potential number of lives that were saved as a result of actions that were put in place. That is why this is important.

As part of our actions we:

- **Identify:** Identify that there is an incident taking place and ensure that this is logged. Record the incident's scope and severity.
- **Report through proper channel:** Alert the people who need to know. Try to contain the problem both technically and also minimizing involvement of staff so that normal operations can proceed. Data/device preservation. Attempt to contain the problem and safeguard your data. Separate affected areas from non-affected areas. Ensure that backups are available if needed and that the company could move over to a hot-site/warm-site/cold site if needed so that normal operations can still resume from there.
- **Use of documentation/documentation changes:** Any and every change made to



the network at this time must be recorded as every change you make moves the network further away from 'business as usual' and the documented network plan. Once the incident is contained you will need to put things back together again, so every step taken will need to be undone later. Also document when and who made the change as we may need permissions to undo these changes later.

- **Chain of custody:** The Forensic first responder's main role, when attending the scene is to secure data about the incident. Data is volatile meaning that it is time-sensitive. PCs may need to be taken away from the scene to be investigated later on using specialist equipment and must be kept powered. For this they are often removed from site in a powered flight case, so that the contents of the RAM are not lost.
- **Copies of data are taken:** The RAM is cloned as is the hard drive. Any other paperwork relevant to the incident may also be taken away. The Forensic investigator will sign a log to state that they are in custody of this evidence. Over time different trained specialists may need to examine the evidence, so the evidence will change hands. Every time it does the log file is updated.
- **Tracking of evidence/documenting process:** The log has to be an unbroken record from the moment the incident took place to the point at which it is presented in court as evidence. If there is a break in the log there is reasonable doubt that the evidence could have been tampered with and therefore the evidence is inadmissible. You need to avoid this at all costs.



# Licensing/DRM/EULA

**Digital Rights Management (DRM)** explains what rights a user has to use a document, or media. If I buy a DVD in the shops I cannot broadcast it in a public place, or an oil rig, but can only use it for my personal pleasure at home. I cannot copy it or resell it, claiming that the material on the disc is my own. DRM protection is built into publicly sold media such as DVDs and also downloaded content, such as from the iTunes store.

A **European User License Agreement (EULA)** is a legally binding contract stating that you abide to the terms of use of the software you are about to install. You can have one active copy on a PC you own, but cannot run multiple copies at the same time.



# Open source versus commercial license

You will find a degree of friction between Microsoft-trained and Linux trained technicians. As an A+ technician you encompass both markets, but the friction is an offshoot from the support due to the type of product both are. Commercial products such as Microsoft Windows have been built through company takeovers, mergers, and the upgrading to code until a sale able product has been put on the market. It is so good that over 85% of commercial companies and home users use it. That is a fact.

However, core code is based on a variation of Open Source software that was created under an Open Source license. Open Source means that you cannot claim that it is your own, but you are part of a collective community and the community can work on and adapt code so long as the adaptation is made available to the rest of the group, eventually public for everybody to use, should they wish to.

Corporately Open Source code is buggy and has no legal guarantee that it will work. This is why a large number of Public Sector companies, especially Local Authority-run schools in the UK refuse to use Open Source software as part of their school network as there is no support for it. In contrast, if Windows does not work as was intended there is an array of support available not to mention a large numbers of updates, hot fixed, and service packs.



# Personal license versus enterprise licenses

I can license a product in one of two ways:

A retail license is where a product key is printed alongside the DVD. When I buy the product in a shop I am allowed to install one instance of the product onto one PC using this product key. The key is registered to me personally.

If you have more than 25 PCs in your network you might want to consider a Key Management Server and an Enterprise License. Here, we buy online as many licenses as we need to use and we are invoiced for this number. License codes are sent to the KMS server, which is basically a catalogue of how many licenses are unused and free. We download the Enterprise edition of the installer (for example, Server 2012 Enterprise edition) and install it on the PC we want to use it on. We are not asked for a key as part of the install, but can supply this either in an unattend.xml file, using System Center, Microsoft Deployment Toolkit, or just by waiting. Once the server is installed, within the first three days the server will try to locate a KMS server and take one license, registering itself as the computer using that license onto the KMS database.

Enterprise licenses can be purchased and attributed to a user, or to a computer. If 100 people use one PC at different times it is cheaper to license the PC than it would be to license the users.





# Personally Identifiable Information

What is your favorite color? What football team do you support? What is your mother's maiden name? What kind of car do you drive? All of these are information about you as an individual, which can be used to identify you. They may be esoteric and not directly related to your name or user account, but may lead someone to identify you.

PII can also include more sensitive data such as your National Insurance number, Date of Birth, Job role, and child's name. The Data Protection Act and its replacement the new General Data Protection Regulation (2018) ensures that companies take care to protect any data held about individuals, which may be used to identify them. A leak of this data can lead to severe fines of up to 20 million euros, or 4% of the companies' total annual worldwide revenue.



# Following corporate end user policies and security best practices

You might not like it, but there will be a good reason why corporate policies are in place. This may be to restrict access to certain websites as they are deemed not productive, or may interfere with normal operations. As a first-line support technician you are not in a position to make a judgment call over what is acceptable; however, you do have to enforce it. Perhaps the policy is in place for a good reason--for example, years ago an IT audit noticed that one department was wasting time by using Facebook, or personal shopping when they should have been working. As a result the company lost money as productivity was down. Perhaps also purchases were being made on company credit cards for personal goods. Action had to be taken because something had happened that needed to be curtailed.

But policy is not law. A policy is a request that you adhere to rules set out by the company. It is not legally enforceable, but is an expectation you are asked to follow.



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide.

- **Prohibited Activity and End User Policies (5:48):** <http://www.professormesser.com/free-a-plus-training/220-902/prohibited-activities-and-end-user-policies/>



## 902.5.4 Demonstrating proper communication techniques and professionalism

We are all different, but in the corporate world there are expectations on how you conduct your conversations. This may be something you already know and do, or this may be new to you. From my experience although some of what follows may seem like common sense, I have met (and include myself in this) a lot of very clever people who know how to fix a computer, but have no regard for their customers. Moreover, they may not be very good at holding a non-technical conversation. For myself, I am a little irascible--I expect other people to already know technical information and it bugs me if I can't have a nerdy conversation as long as I am not out-nerded!

I am very proud that recently one of my students, a teenager with Asperger's Syndrome, a Linux fan, and not a Microsoft fan at all, had to be convinced not only to embrace the dark side, but also how to dress correctly when visiting a customer. He not only passed A+, but aced the exams and now works in the industry.

There is a stereotype over IT technicians personified with the three characters in the TV series The IT Crowd: The uncaring Roy, the geeky Moss, and Richmond the Goth vampire! Reality is quite different from this--most IT Managers have a Computing Degree or have moved across into IT. Open Source software is used when it is considered the best fit for the project and the network grows organically based on need.

The main point to note is that when a customer presents a problem they are asking for your help. They own the problem--you are facilitating, assisting them with the fix in the same way that if you need work done on your car you will go to a repair garage and the mechanic will help you by fixing the problem, but it is still your car.

- **Use proper language:** Avoid jargon, acronyms, and slang when applicable--most end users are not IT-savvy, so every keyword I have referred to in this book will probably be alien to them. We therefore describe the issue using non-technical language, keeping to the facts, and allowing the end-user to make decisions as to what remediation needs to take place.
- **Maintain a positive attitude/project confidence:** It may be hard when you learn the extent of a problem to keep a positive outlook, but projecting confidence is a

skill that will put your end-user at ease. Any challenge you are presented with can be overcome and as a technician I enjoy the challenges presented to me.

"Life is about accepting the challenges along the way, choosing to keep moving forward, and savoring the journey."—Roy T. Bennett, *The Light in the Heart*

- **Actively listen (taking notes) and avoid interrupting the customer:** There is a specific technique to follow, especially when taking an initial call on the phone from a customer who is trying to identify a problem to you. Use open questions to try to coax them to speak more about what has happened, but when you need specific detail use closed questions (ones which require a short, or yes/no answer) to narrow the line of questioning, pinpointing the exact nature of the problem. Do take notes as they may reveal something that is quite relevant, but not realize the importance of it. Allow the customer to continue with their conversation otherwise your interruption, as well as being rude, may break their train of thought and they may then neglect to provide other information, which may be important to your investigation.
- **Be culturally sensitive:** The person may be upset that the incident has happened. They may also have expectations that do not match yours. Their attitude might be you're IT - it's your problem; however, don't let that annoy you. In reality they cannot perform the fix otherwise they wouldn't have come to you. You are providing a service to the company as a whole by fixing the problem.

Good customer service is not only keeping a professional outlook when dealing with customers, but seeing a job through to its completion in a timely manner and getting back to the customer to advise them how the fix is going, or to let them know that the problem has been resolved. You may even want to show the customer a few tips to help them avoid the problem occurring again:

- **Use appropriate professional titles, when applicable:** Address the customer as Mr/Mrs/Miss/Ms and do not address them by their first name even if they do to you until they allow you to use their first name.
- **Be on time (if late contact the customer):** Exactly that. Have the customer's contact number and try to be there 15 minutes before the agreed time to give yourself time to park, or to freshen up. You may only be arriving to fix a PC, but treat it as a business meeting. You are looking to give a good impression because when the problem has been solved the customer may report back to your Line Manager on what a good job you have done.





As part of our training courses I provide a course completion certificate to every delegate, also an evaluation form and encourage positive feedback. I invite the delegate to also leave a testimonial should they wish to and get permission for us to use this testimonial in our online marketing. That reflects well as when we then post our testimonials on LinkedIn and Twitter we often get very positive feedback from our audience, some of whom may be looking to buy courses themselves.

- **Avoid distractions:** Try to keep your mind on the job not only to ensure that the fix occurs in a timely manner, but also it is off-putting for you and shows a lack of professionalism because your mind is not on the job.

When I am fixing a PC I put my personal phone on silent to avoid taking a personal call whilst working. If I am expecting a call I mention this to the customer and ask if it would be OK for me to answer it if it rings, if this is an expected professional call concerning another job, but as a rule I stick to the job at hand.

Equally I do not use social media sites, or browse the internet while I am waiting for an installation to complete. I avoid chatting with co-workers as you will put them off their work and should be devoting your time to your customer.



# Dealing with difficult customers or situations

Sadly, this does happen. The customer is annoyed because IT has let them down and believes that your role is to fix the problem. Angry customers are not necessarily angry at you, but frustrated with what has happened and just want the problem to go away.

- **Do not argue with customers and/or be defensive:** There is a likelihood that the customer may personalize their anger by asking you what you are going to do to fix the problem. They may have an idea as to what actually needs fixing and this idea may not be realistic. It is best to inform the customer with what needs to happen and a timescale so that they can mentally plan for this. Stay objective and reassure them that you will do your best to resolve the problem, but try not to be unrealistic. For example, if you need to buy a part and you have to wait for delivery explain this to the customer and possibly try to source a replacement PC for them to use in the interim.
- **Avoid dismissing customer problems:** A customer may dwell on one aspect of the problem. They need to know that you accept what they say, whether this is correct or not, and explain some of the other factors as well that will need to be looked into. For example, if a PC is infected by a virus, the actions the virus were seen by the user to have performed may only form a very small amount of damage actually inflicted and not in itself indicative of the work you will have to do. The customer will probably not have taken a system image themselves so you may have to rebuild the image from scratch. Avoid being judgmental. Don't blame the customer for what has happened--things happen. The customer may now show it, but may already be blaming themselves for what has happened. If, for example, a virus infected their PC due to a website they visited, or a spam email they opened that contained a Trojan attachment, they will already be feeling very guilt-ridden and uncertain if there will be any repercussions for their actions. They may, or may not be, but that is a decision for someone else. Your job is to fix the immediate problem.
- **Clarify customer statements (ask open-ended questions to narrow the scope of the problem, restate the issue, or question to verify understanding):** I often repeat what the customer said to me. I let them finish their point and then recap by starting with: OK, so what you are telling me is that..... This way we get agreement on the facts stated by both parties. The customer may not be able to describe a

problem using technical language because they don't know it. This is why IT often frustrates end users. However, you need the facts to ensure that you know what has happened, why it has happened, and the extent of the damage.

- **Do not disclose experiences via social media outlets:** The internet is a cruel place. Anything you say on the internet will be around for some time and may even be used as evidence. It is therefore bad practice to comment on something your customer has done or said because other people may potentially also be your customers. Do you think they will want to work with you if you are going to disclose something about them? A competitor may also know what work you have been doing. Do you really want to make this information public? As a rule, if you are happy to shout the same information in the street for passers-by to hear then you can post it online.



# **Setting and meeting expectations/timeline and communicate status with the customer**

As mentioned previously, the customer's expectations and timescale, also repair costs might not be realistic. If you can do so, offer different repair/replacement options if applicable. Give them choices--this empowers them.

As the customer will need to make a decision provide them with product specifications and prices so that they can make an informed choice. Of course, they will ask you for your opinion. Provide proper documentation on the services provided.

Once the job is done you may need to set the equipment up for them in-suit. This is a good time to provide post-fix support and any end-user training to make their use of the equipment more effective. If you have replaced a PC and their new PC is more powerful or has new features this would be a good time to showcase the extra features. You are turning what has been for the customer a frustrating time into something fun and positive.

It doesn't hurt to check back with the customer a few days, or a week later. Follow up with customers/users at a later date to verify satisfaction



# **Dealing appropriately with customers confidential and private materials**

This is more relevant when you are at an office desk, or servicing a PC in a customer's home. You will see information that is confidential and have to learn to ignore it. You may see this in the form of passwords or telephone numbers on post-it notes, letters and bank statements, or printed documents still in the printer out tray. If you are caught reading these, even though the data may not be relevant to you, do you think the customer will continue to trust you?





# Safeguarding

Although not in the exam objectives this does come up regularly in the A+ exam. Imagine the scenario where you are working in someone's home. They have a small child playing in the house. The customer states that they need to pop out for a few minutes. What do you do?

You don't have the duty of care for the child and could be accused of ill-treating the child should anything happen to it while the customer is away. As you want to avoid this from happening the correct thing to do would be to stop the repair work you are doing and re-arrange another time where you can continue the repair work. It might be a simple case to say that you need to take a lunch break, or phone the office in your car, but need to leave the premises for a short while. Agree with the customer when to return to continue with the repair. This way you avoid the problem.



# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **Communication (4:13):** <http://www.professormesser.com/free-a-plus-training/220-902/communication-2/>
- **Professionalism (4:12):** <http://www.professormesser.com/free-a-plus-training/220-902/professionalism-2/>



## 902.5.5 Given a scenario, explain the troubleshooting theory

CompTIA has a six-step process to follow when performing a fix. The exam will have a series of questions based on a scenario and will mention an activity taking place. You have to decide which stage is being described in the question.

Always consider corporate policies, procedures, and impacts before implementing changes:

- **Identify the problem:** Question the user and identify user changes to computer and perform backups before making changes
- **Establish a theory of probable cause (question the obvious):** If necessary, conduct external or internal research based on symptoms
- **Test the theory to determine cause:** Once a theory is confirmed, determine next steps to resolve problem--if theory is not confirmed, re-establish new theory or escalate
- Establish a plan of action to resolve the problem and implement the solution
- Verify full system functionality and if applicable implement preventive measures
- Document findings, actions, and outcomes



# Exam questions

1. What measures would you take to keep yourself safe when dismantling a PC?
  - Answer:
2. Why should you not wear jewellery when working with a PC?
  - Answer:
3. Why should you not wear a tie when working with a photocopier, or print device?
  - Answer:
4. Name some of the information held on a Materials Safety Data sheet:
  - Answer:
5. A user has bought a book on their Kindle using a company account. The book is going to be used for business uses and the purchase was approved by their manager. The book is on a limited purchase of 30 days. What IT principle is this?
  - Answer:
6. A contractor is chatting to a member of staff in the kitchen. They are talking about their favorite TV program in a great degree of detail. What information is being disclosed that could be used against the user at a future point?
  - Answer:
7. Why should we avoid using jargon?
  - Answer:
8. Describe active listening:
  - Answer:
9. Why should you never argue with a customer, even though I know that I am right?
  - Answer:
10. What is the final thing you should do after you have completed work on a problem?
  - Answer:





# Video training

To summarize this section, I recommend that you review the points made here by referring to the Professor Messer series of videos available at <http://www.professormesser.com>. James Messer's training series is quick, easy to understand, and provides an excellent overview and accompaniment to this study guide:

- **How to Troubleshoot (4:42):** <http://www.professormesser.com/free-a-plus-training/220-902/how-to-troubleshoot/>



# Summary

This chapter has detailed some of the safety measures you should take to protect the hardware from damage as well as yourself from shock. Never take shortcuts and be sure to use the right tools. Always have a separate workbench that is well lit and with plenty of space as you will be looking to place components you have removed in order. Have anti-static bags for circuitry to ensure that they do not receive a static shock. Use a grounding mat, plug, and wrist strap to eliminate static. Always use the correct tools. Put your screws into groups based on what they are used for, or in a screw pot. Never over-tighten screws otherwise you will damage the head and threads. Think about your personal safety - is the room secure? Are there any trailing cables or anything you might trip over? Are you obscuring the way for others?

When working with toner remember to wear a breathing mask. When working with extreme light sources, especially with a laser from a DVD drive, be sure to wear protective goggles and not to look directly at the source of light.

Consider power usage - how do we protect the device from damage in the case of a surge? Do we need to condition the line to ensure that power flows equally? Do we need an alternative source of power? A battery? A UPS box for the server? Possibly a generator if we are 'off-grid' or if the mains power will be unavailable for a long time.

Consider temperature and humidity. Do you have filters and air-conditioning in place that ensures a smooth running of the equipment? If stored in racks, have you set up hot and cold airflow zones?

Finally, in relation to Forensics have you ensured that corporately your company has a policy to follow and trained staff to be Forensic First Responders? These may conflict with the IT team's agenda of containment and to fix the fault as quickly as possible. Here we looked at security best practice such as the Chain of Custody.

Have you considered rich media and other documents that are protected through Rights Management? Have you considered non-technical information about a person that could be used to 'spear' a phishing, or vishing attack, and how to train your end-users not to provide personal information to people they do not know?

We also looked at the concept of Professionalism and I identified what I consider to be good practice here, in line with CompTIA's objectives. This looked at the 'soft skills' -

customer expectations, who the problem owner is, keeping information about your work within the company, and not reporting issues publicly on social media.

Finally, we covered CompTIA's six-step troubleshooting theory. The exam will give you a scenario and you will have to work out which stage of the process is being described.



# Finale

And there we have it. This book is possibly the most concise CompTIA A+ guide on the market. I have tried to not get too technical and you will see that the practical examples explaining how to perform certain tasks have not featured in here. The reason for this is that I want you to focus on the theory aspect of A+.

I expect you to be able to do the myriad of things described here from a practical level - experience is key and that only comes once you have fixed a few PCs.

One student once asked me at what point they would be qualified to take a PC apart. It doesn't work like that. I worked as an IT technician back in the 1990s building up a reputation from word of mouth. I used to also recondition and resell Dell Optiplex PCs. I learned how to fix faults just by being there, through research and experimentation. I then signed up to take the MCSA Server 2003 course and didn't understand very much of the protocols and concepts at first, but after I had applied them I started to realize how it all fitted together.

I worked in a school and got to learn what a server was. This was before the days of Hyper-V and it wasn't until much later that I was able to make my own Enterprise network, virtually, at home.

I'm a very literal and pragmatic person and not great in dealing with end-users. End-users often annoy me because they don't play by the rules and tend to break things. I have learned that the best thing to do is to stay silent, smile, remember why you are there, and that you are being paid to fix other people's problems. I then remembered that I wouldn't always fix faults as I had aspirations to move on to more senior, advanced support. I now focus on teaching and solving Cyber Security issues. My company (I am the Director and owner of MBIT Training Ltd: <https://mbittrainingltd.com/en/>) support and work with the National Cyber Security Center and offer corporate training to a variety of customers including the US Air Force. I could not have dreamt for a better outcome and certainly have surpassed my initial aims.

You too also need to have an aim. For this I recommend that you visit CompTIA's roadmap. The details page is here (<https://certification.comptia.org/why-certify/roadmap>) and I also recommend this tube map that shows you what you need to obtain a particular job and get to a certain level (<https://certification.comptia.org/docs/default-source/downloadablefiles/it-certification-roadmap.pdf>) .

So, what happens now? In this book I have provided approx 120 practice test questions used to confirm your knowledge. Aim to get 80% of these right without having to look up the answers. If necessary you might like to take an online practice test, such as [Measure up.Com](#). Here, take the test in certification mode and get 80%--twice, before booking your test.

Now that you know that you are ready you need to buy the exam voucher. This can be bought from <http://www.comptiastore.co.uk/ProductDetails.asp?ProductCode=comptiaa> and at the time of writing the cost is £120 per exam (remember--you have two exams to take!).

Once you have passed both exams, register at <https://www.certmetrics.com/comptia/login.aspx> to create a CompTIA account. Create a transcript (this is like an online CV and can be shared with employees and potential employees and is used to check that you actually have passed the exam) by using this link: <https://certification.comptia.org/help/certificates-credentials-transcripts/credentials/create-a-transcript>. You should see your two passes and overall A+ certificate, which you can download as a PDF and also request a hard copy be sent to you along with a wallet ID card.

A+ is a Continuing Education certificate. This means that as things change over time there will be new concepts and technologies in the next exam, which will be in three years time. If you decide to upgrade, for example take the Network+ exam next, when you pass this you automatically get other lower-level exams (for example, A+) automatically renewed.

Finally one tip: The account you use to register to create your CompTIA account should be a professional looking but personal email address. Do not use your work email as this may change over time and if you leave your employer you still need to access the CompTIA account. I took a lot of Microsoft exams after completing my A+, so not only used the same email address for both accounts, but associated my Microsoft account to my CompTIA account and vice versa. That way both sets of exam results appear on both my CompTIA and Microsoft transcripts. This makes HR's job a lot easier when you come to take that new job.

I do hope that this book has been enjoyable. I want to thank you for taking the time to study what I hope has been a thoughtful and interesting course and hope to meet you in person in the field, keeping the lights on and the IT working.





# Processor Table

List of 80x86 sockets and slots

**Table legend:**

Intel only

AMD only

Socket name	Year of introduction	CPU families supported	Computer type	Package	Pin count	Bus clock and transfers	N
Socket 7 ( <a href="https://en.wikipedia.org/wiki/Socket_7">https://en.wikipedia.org/wiki/Socket_7</a> )	1994	Intel Pentium P5 ( <a href="https://en.wikipedia.org/wiki/P5_(microarchitecture)">https://en.wikipedia.org/wiki/P5_(microarchitecture)</a> ) Intel Pentium MMX ( <a href="https://en.wikipedia.org/wiki/P5_(microarchitecture)#MMX">https://en.wikipedia.org/wiki/P5_(microarchitecture)#MMX</a> ) AMD ( <a href="https://en.wikipedia.org/wiki/Advanced_Micro_Devices">https://en.wikipedia.org/wiki/Advanced_Micro_Devices</a> ) K6 ( <a href="https://en.wikipedia.org/wiki/AMD_K6">https://en.wikipedia.org/wiki/AMD_K6</a> )		PGA	321	50–66 MHz	It uses Pin Socket architecture of serial parallel operation
		AMD K6-2 ( <a href="https://en.wikipedia.org/wiki/AMD_K6-2">https://en.wikipedia.org/wiki/AMD_K6-2</a> ) AMD K6-					

<b>Super Socket 7</b> ( <a href="https://en.wikipedia.org/wiki/Super_Socket_7">https://en.wikipedia.org/wiki/Super_Socket_7</a> )	1998	III ( <a href="https://en.wikipedia.org/wiki/AMD_K6-III">https://en.wikipedia.org/wiki/AMD_K6-III</a> ) Rise ( <a href="https://en.wikipedia.org/wiki/Rise_Technology">https://en.wikipedia.org/wiki/Rise_Technology</a> ) mP6 ( <a href="https://en.wikipedia.org/wiki/MP6">https://en.wikipedia.org/wiki/MP6</a> ) Cyrix MII ( <a href="https://en.wikipedia.org/wiki/Cyrix_6x86">https://en.wikipedia.org/wiki/Cyrix_6x86</a> )		PGA	321	66–100 MHz	B c S S p
<b>Socket 8</b> ( <a href="https://en.wikipedia.org/wiki/Socket_8">https://en.wikipedia.org/wiki/Socket_8</a> )	1995	Intel Pentium Pro ( <a href="https://en.wikipedia.org/wiki/Pentium_Pro">https://en.wikipedia.org/wiki/Pentium_Pro</a> )		PGA	387	60–66 MHz	
<b>Slot 1</b> ( <a href="https://en.wikipedia.org/wiki/Slot_1">https://en.wikipedia.org/wiki/Slot_1</a> )	1997	Intel Pentium II ( <a href="https://en.wikipedia.org/wiki/Pentium_II">https://en.wikipedia.org/wiki/Pentium_II</a> ) Intel Pentium III ( <a href="https://en.wikipedia.org/wiki/Pentium_III">https://en.wikipedia.org/wiki/Pentium_III</a> )		Slot	242	66–133 MHz	C (C M P (F D P (F v P (c
<b>Slot 2</b> ( <a href="https://en.wikipedia.org/wiki/Slot_2">https://en.wikipedia.org/wiki/Slot_2</a> )	1998	Intel Pentium II Xeon ( <a href="https://en.wikipedia.org/wiki/Xeon#Pentium_II_Xeon">https://en.wikipedia.org/wiki/Xeon#Pentium_II_Xeon</a> )		Slot	330	100–133 MHz	

<b>Socket 463/ Socket NexGen</b>	1994	NexGen ( <a href="https://en.wikipedia.org/wiki/NexGen">https://en.wikipedia.org/wiki/NexGen</a> )  Nx586 ( <a href="https://en.wikipedia.org/wiki/NexGen">https://en.wikipedia.org/wiki/NexGen</a> )		PGA	463	37.5–66MHz
<b>Socket 587</b>	1995	Alpha 21164A ( <a href="https://en.wikipedia.org/wiki/Alpha_21164">https://en.wikipedia.org/wiki/Alpha_21164</a> )		Slot	587	?
<b>Slot A</b> ( <a href="https://en.wikipedia.org/wiki/Slot_A">https://en.wikipedia.org/wiki/Slot_A</a> )	1999	AMD ( <a href="https://en.wikipedia.org/wiki/Advanced_Micro_Devices">https://en.wikipedia.org/wiki/Advanced_Micro_Devices</a> )  Athlon ( <a href="https://en.wikipedia.org/wiki/Athlon">https://en.wikipedia.org/wiki/Athlon</a> )		Slot	242	100 MHz
<b>Slot B</b>	?	Alpha 21264 ( <a href="https://en.wikipedia.org/wiki/Alpha_21264">https://en.wikipedia.org/wiki/Alpha_21264</a> )		Slot	587	?
		Intel Pentium III ( <a href="https://en.wikipedia.org/wiki/Pentium_III">https://en.wikipedia.org/wiki/Pentium_III</a> ) Intel Celeron ( <a href="https://en.wikipedia.org/wiki/Celeron">https://en.wikipedia.org/wiki/Celeron</a> )				

<b>Socket 370</b> ( <a href="https://en.wikipedia.org/wiki/Socket_370">https://en.wikipedia.org/wiki/Socket_370</a> )	1999	VIA ( <a href="https://en.wikipedia.org/wiki/VIA_Technologies">https://en.wikipedia.org/wiki/VIA_Technologies</a> ) Cyrix III ( <a href="https://en.wikipedia.org/wiki/Cyrix_III">https://en.wikipedia.org/wiki/Cyrix_III</a> ) VIA ( <a href="https://en.wikipedia.org/wiki/VIA_Technologies">https://en.wikipedia.org/wiki/VIA_Technologies</a> ) C3 ( <a href="https://en.wikipedia.org/wiki/VIA_C3">https://en.wikipedia.org/wiki/VIA_C3</a> )		PGA	370	66–133 MHz	
<b>Socket A</b> ( <a href="https://en.wikipedia.org/wiki/Socket_A">https://en.wikipedia.org/wiki/Socket_A</a> )/ <b>Socket 462</b>	2000	AMD Athlon AMD Duron AMD Athlon XP AMD Athlon XP-M AMD Athlon MP AMD Sempron	Desktop	PGA	462	100–200 MHz 400 MT/s[lower-alpha 1] ( <a href="https://en.wikipedia.org/wiki/CPU_socket#cite_note-dbl_rate-2">https://en.wikipedia.org/wiki/CPU_socket#cite_note-dbl_rate-2</a> )	
<b>Socket 423</b> ( <a href="https://en.wikipedia.org/wiki/Socket_423">https://en.wikipedia.org/wiki/Socket_423</a> )	2000	Intel Pentium 4 ( <a href="https://en.wikipedia.org/wiki/Pentium_4">https://en.wikipedia.org/wiki/Pentium_4</a> )	Desktop	PGA	423	100 MHz 400 MT/s	W o: C o: C a
		Intel Pentium 4 ( <a href="https://en.wikipedia.org/wiki/">https://en.wikipedia.org/wiki/</a> )					

<b>Socket 478</b> ( <a href="https://en.wikipedia.org/wiki/Socket_478/">https://en.wikipedia.org/wiki/Socket_478/</a> ) <b>Socket N</b> ( <a href="https://en.wikipedia.org/wiki/Socket_478">https://en.wikipedia.org/wiki/Socket_478</a> )	2000	<a href="#">Pentium_4</a> Intel Celeron ( <a href="https://en.wikipedia.org/wiki/Celeron">https://en.wikipedia.org/wiki/Celeron</a> ) Intel Pentium 4 EE ( <a href="https://en.wikipedia.org/wiki/Pentium_4#Extreme_Edition">https://en.wikipedia.org/wiki/Pentium_4#Extreme_Edition</a> ) Intel Pentium 4 M ( <a href="https://en.wikipedia.org/wiki/List_of_Intel_Pentium_4_microprocessors#Mobile_processors">https://en.wikipedia.org/wiki/List_of_Intel_Pentium_4_microprocessors#Mobile_processors</a> )	Desktop	PGA	478	100–200 MHz 400–800 MT/s
<b>Socket 495</b> ( <a href="https://en.wikipedia.org/wiki/Socket_495">https://en.wikipedia.org/wiki/Socket_495</a> )	2000	Intel Celeron Intel Pentium III	Notebook	PGA	495	66–133MHz
<b>PAC418</b> ( <a href="https://en.wikipedia.org/wiki/PAC418">https://en.wikipedia.org/wiki/PAC418</a> )	2001	Intel Itanium ( <a href="https://en.wikipedia.org/wiki/Itanium">https://en.wikipedia.org/wiki/Itanium</a> )		PGA	418	133 MHz
<b>Socket 603</b> ( <a href="https://en.wikipedia.org/wiki/Socket_603">https://en.wikipedia.org/wiki/Socket_603</a> )	2001	Intel Xeon ( <a href="https://en.wikipedia.org/wiki/Xeon">https://en.wikipedia.org/wiki/Xeon</a> )	Server	PGA	603	100–133 MHz 400–533 MT/s

<b>Socket 563</b> ( <a href="https://en.wikipedia.org/wiki/Socket_563">https://en.wikipedia.org/wiki/Socket_563</a> )	2002	AMD Athlon ( <a href="https://en.wikipedia.org/wiki/Athlon">https://en.wikipedia.org/wiki/Athlon</a> ) XP-M	Notebook	PGA	563	?
<b>PAC611</b> ( <a href="https://en.wikipedia.org/wiki/PAC611">https://en.wikipedia.org/wiki/PAC611</a> )	2002	Intel Itanium 2 ( <a href="https://en.wikipedia.org/wiki/Itanium#Itanium_2:_2002.E2.80.932010">https://en.wikipedia.org/wiki/Itanium#Itanium_2:_2002.E2.80.932010</a> ) HP ( <a href="https://en.wikipedia.org/wiki/Hewlett-Packard">https://en.wikipedia.org/wiki/Hewlett-Packard</a> ) PA-8800 ( <a href="https://en.wikipedia.org/wiki/PA-8000">https://en.wikipedia.org/wiki/PA-8000</a> ), PA-8900 ( <a href="https://en.wikipedia.org/wiki/PA-8000">https://en.wikipedia.org/wiki/PA-8000</a> )		PGA	611	?
<b>Socket 604</b> ( <a href="https://en.wikipedia.org/wiki/Socket_604">https://en.wikipedia.org/wiki/Socket_604</a> )	2002	Intel Xeon ( <a href="https://en.wikipedia.org/wiki/Xeon">https://en.wikipedia.org/wiki/Xeon</a> )	Server	PGA	604	100–266 MHz 400–1066 MT/s
<b>Socket 754</b> ( <a href="https://en.wikipedia.org/wiki/Socket_754">https://en.wikipedia.org/wiki/Socket_754</a> )	2003	AMD Athlon 64 ( <a href="https://en.wikipedia.org/wiki/Athlon_64">https://en.wikipedia.org/wiki/Athlon_64</a> ) AMD Sempron ( <a href="https://en.wikipedia.org/wiki/Sempron">https://en.wikipedia.org/wiki/Sempron</a> )	Desktop	PGA	754	200–800 MHz

		AMD Turion 64 ( <a href="https://en.wikipedia.org/wiki/AMD_Turion">https://en.wikipedia.org/wiki/AMD_Turion</a> )					
<b>Socket 940</b> ( <a href="https://en.wikipedia.org/wiki/Socket_940">https://en.wikipedia.org/wiki/Socket_940</a> )	2003	AMD Opteron ( <a href="https://en.wikipedia.org/wiki/Opteron">https://en.wikipedia.org/wiki/Opteron</a> ) Athlon 64 FX ( <a href="https://en.wikipedia.org/wiki/Athlon_64#Athlon_64_FX">https://en.wikipedia.org/wiki/Athlon_64#Athlon_64_FX</a> )	Server Desktop	PGA ( <a href="https://en.wikipedia.org/wiki/Pin_grid_array">https://en.wikipedia.org/wiki/Pin_grid_array</a> )	940	200–1000 MHz	
<b>Socket 479</b> ( <a href="https://en.wikipedia.org/wiki/Socket_479">https://en.wikipedia.org/wiki/Socket_479</a> )	2003	Intel Pentium M ( <a href="https://en.wikipedia.org/wiki/Pentium_M">https://en.wikipedia.org/wiki/Pentium_M</a> ) Intel Celeron M ( <a href="https://en.wikipedia.org/wiki/Celeron#Celeron_M">https://en.wikipedia.org/wiki/Celeron#Celeron_M</a> )	Notebook	PGA	479[1] ( <a href="https://en.wikipedia.org/wiki/CPUs_socket#cite_note-479note-9">https://en.wikipedia.org/wiki/CPUs_socket#cite_note-479note-9</a> )	100–133 MHz 400–533 MT/s	
<b>Socket 939</b> ( <a href="https://en.wikipedia.org/wiki/Socket_939">https://en.wikipedia.org/wiki/Socket_939</a> )	2004	AMD Athlon 64 ( <a href="https://en.wikipedia.org/wiki/Athlon_64">https://en.wikipedia.org/wiki/Athlon_64</a> ) AMD Athlon 64 FX ( <a href="https://en.wikipedia.org/wiki/Athlon_64#Athlon_64_FX">https://en.wikipedia.org/wiki/Athlon_64#Athlon_64_FX</a> ) AMD Athlon 64	Desktop	PGA	939	200–1000 MHz	S A p s i k i 6 4 S O



39)		<p>X2 (<a href="https://en.wikipedia.org/wiki/Athlon_64_X2">https://en.wikipedia.org/wiki/Athlon_64_X2</a>)</p> <p>AMD</p> <p>Opteron (<a href="https://en.wikipedia.org/wiki/Opteron">https://en.wikipedia.org/wiki/Opteron</a>)</p>					wi er 10
<p><b>LGA 775</b> (<a href="https://en.wikipedia.org/wiki/LGA_775">https://en.wikipedia.org/wiki/LGA_775</a>)/</p> <p><b>Socket T</b></p>	2004	<p>Intel Pentium 4 (<a href="https://en.wikipedia.org/wiki/Pentium_4">https://en.wikipedia.org/wiki/Pentium_4</a>)</p> <p>Intel Pentium D (<a href="https://en.wikipedia.org/wiki/Pentium_D">https://en.wikipedia.org/wiki/Pentium_D</a>)</p> <p>Intel Celeron (<a href="https://en.wikipedia.org/wiki/Celeron">https://en.wikipedia.org/wiki/Celeron</a>)</p> <p>Intel Celeron D (<a href="https://en.wikipedia.org/wiki/Celeron#Celeron_D">https://en.wikipedia.org/wiki/Celeron#Celeron_D</a>)</p> <p>Intel Pentium XE (<a href="https://en.wikipedia.org/wiki/Pentium_D#Pentium_Extreme_Edition">https://en.wikipedia.org/wiki/Pentium_D#Pentium_Extreme_Edition</a>)</p> <p>Intel Core 2 Duo (<a href="https://en.wikipedia.org/wiki/Intel_Core#Core_2_Duo">https://en.wikipedia.org/wiki/Intel_Core#Core_2_Duo</a>)</p> <p>Intel Core</p>	Desktop	<p>LGA (<a href="https://en.wikipedia.org/wiki/Land_grid_array">https://en.wikipedia.org/wiki/Land_grid_array</a>)</p>	775	1600 MHz	C 7' sl n: us

		2 Quad ( <a href="https://en.wikipedia.org/wiki/Intel_Core#Core_2_Quad">https://en.wikipedia.org/wiki/Intel_Core#Core_2_Quad</a> ) Intel Xeon ( <a href="https://en.wikipedia.org/wiki/Xeon">https://en.wikipedia.org/wiki/Xeon</a> )					
<b>Socket M</b> ( <a href="https://en.wikipedia.org/wiki/Socket_M">https://en.wikipedia.org/wiki/Socket_M</a> )	2006	Intel Core Solo ( <a href="https://en.wikipedia.org/wiki/Intel_Core#Core_Solo">https://en.wikipedia.org/wiki/Intel_Core#Core_Solo</a> ) Intel Core Duo ( <a href="https://en.wikipedia.org/wiki/Intel_Core#Core_Duo">https://en.wikipedia.org/wiki/Intel_Core#Core_Duo</a> ) Intel Dual-Core Xeon ( <a href="https://en.wikipedia.org/wiki/Xeon">https://en.wikipedia.org/wiki/Xeon</a> ) Intel Core 2 Duo ( <a href="https://en.wikipedia.org/wiki/Intel_Core#Core_2_Duo">https://en.wikipedia.org/wiki/Intel_Core#Core_2_Duo</a> )	Notebook	PGA	478	133–166 MHz 533–667 MT/s	R 4' <a href="#">ed</a> 79
<b>LGA 771</b> ( <a href="https://en.wikipedia.org/wiki/LGA_771">https://en.wikipedia.org/wiki/LGA_771</a> )/ <b>Socket J</b>	2006	Intel Xeon ( <a href="https://en.wikipedia.org/wiki/Xeon">https://en.wikipedia.org/wiki/Xeon</a> )	Server	LGA ( <a href="https://en.wikipedia.org/wiki/Land_grid_array">https://en.wikipedia.org/wiki/Land_grid_array</a> )	771	1600MHz	S 7' al
<b>Socket S1</b> ( <a href="https://en.wikipedia.org/wiki/Socket_S1">https://en.wikipedia.org/wiki/Socket_S1</a> )	2006	AMD Turion 64 X2 ( <a href="https://en.wikipedia.org/wiki/Turion_64_X2">https://en.wikipedia.org/wiki/Turion_64_X2</a> )	Notebook	PGA	638	200–800	

<a href="#">dia.org/wiki/Socket_S1)</a>		<a href="#">n.wikipedia.org/wiki/AMD_Turion)</a>				MHz	
<b>Socket AM2</b> ( <a href="https://en.wikipedia.org/wiki/Socket_AM2">https://en.wikipedia.org/wiki/Socket_AM2</a> )	2006	AMD Athlon 64 ( <a href="https://en.wikipedia.org/wiki/Athlon_64">https://en.wikipedia.org/wiki/Athlon_64</a> ) AMD Athlon 64 X2 ( <a href="https://en.wikipedia.org/wiki/Athlon_64_X2">https://en.wikipedia.org/wiki/Athlon_64_X2</a> )	Desktop	PGA ( <a href="https://en.wikipedia.org/wiki/Pin_grid_array">https://en.wikipedia.org/wiki/Pin_grid_array</a> )	940	200–1000 MHz	R 7: 9:
<b>Socket F</b> ( <a href="https://en.wikipedia.org/wiki/Socket_F">https://en.wikipedia.org/wiki/Socket_F</a> )/ <b>Socket L (Socket 1207FX)</b>	2006	AMD Athlon 64 FX ( <a href="https://en.wikipedia.org/wiki/Athlon_64#Athlon_64_FX">https://en.wikipedia.org/wiki/Athlon_64#Athlon_64_FX</a> ) AMD Opteron ( <a href="https://en.wikipedia.org/wiki/Opteron">https://en.wikipedia.org/wiki/Opteron</a> ) (Socket L only support Athlon 64 FX)	Server Desktop	LGA ( <a href="https://en.wikipedia.org/wiki/Land_grid_array">https://en.wikipedia.org/wiki/Land_grid_array</a> )	1207	? Socket L: 1000 MHz in Single CPU mode, 2000 MHz in Dual CPU mode	R 9: <a href="#">ed</a> 40 S in ei w p d ju S d sp ai oi in L M
		AMD Athlon 64 ( <a href="https://en.wikipedia.org/wiki/Athlon_64">https://en.wikipedia.org/wiki/Athlon_64</a> ) AMD					S p

<b>Socket AM2+ (</b> ( <a href="https://en.wikipedia.org/wiki/Socket_AM2+">https://en.wikipedia.org/wiki/Socket_AM2+</a> )	2007	Athlon X2 ( <a href="https://en.wikipedia.org/wiki/Athlon_64_X2#Athlon_X2">https://en.wikipedia.org/wiki/Athlon_64_X2#Athlon_X2</a> ) AMD Phenom ( <a href="https://en.wikipedia.org/wiki/AMD_Phenom">https://en.wikipedia.org/wiki/AMD_Phenom</a> ) AMD Phenom II ( <a href="https://en.wikipedia.org/wiki/Phenom_II">https://en.wikipedia.org/wiki/Phenom_II</a> )	Desktop	PGA ( <a href="https://en.wikipedia.org/wiki/Pin_grid_array">https://en.wikipedia.org/wiki/Pin_grid_array</a> )	940	200–2600 MHz	R A p e A C in A c S
<b>Socket P (</b> ( <a href="https://en.wikipedia.org/wiki/Socket_P">https://en.wikipedia.org/wiki/Socket_P</a> )	2007	Intel Core 2 ( <a href="https://en.wikipedia.org/wiki/Intel_Core_2">https://en.wikipedia.org/wiki/Intel_Core_2</a> )	Notebook	PGA	478	133–266 MHz 533–1066 MT/s	R M ia.
<b>Socket 441 (</b> ( <a href="https://en.wikipedia.org/wiki/Socket_441">https://en.wikipedia.org/wiki/Socket_441</a> )	2008	Intel Atom ( <a href="https://en.wikipedia.org/wiki/Intel_Atom">https://en.wikipedia.org/wiki/Intel_Atom</a> )	Sub-notebook	PGA	441	400–667 MHz	
<b>LGA 1366 (</b> ( <a href="https://en.wikipedia.org/wiki/LGA_1366">https://en.wikipedia.org/wiki/LGA_1366</a> )/ <b>Socket B</b>	2008	Intel Core i7 ( <a href="https://en.wikipedia.org/wiki/List_of_Intel_Core_i7_microprocessors">https://en.wikipedia.org/wiki/List_of_Intel_Core_i7_microprocessors</a> ) (900 series) Intel Xeon (35xx, 36xx, 55xx, 56xx series)	Server	LGA ( <a href="https://en.wikipedia.org/wiki/Land_grid_array">https://en.wikipedia.org/wiki/Land_grid_array</a> )	1366	4.8–6.4 GT/s	R J th

<p><b>rPGA 988A</b> (<a href="https://en.wikipedia.org/wiki/Socket_G1/">https://en.wikipedia.org/wiki/Socket_G1/</a>) <b>Socket G1</b></p>	<p>2008</p>	<p>Intel Core i7 (<a href="https://en.wikipedia.org/wiki/List_of_Intel_Core_i7_microprocessors">https://en.wikipedia.org/wiki/List_of_Intel_Core_i7_microprocessors</a>) (600, 700, 800, 900 series) Intel Core i5 (<a href="https://en.wikipedia.org/wiki/List_of_Intel_Core_i5_microprocessors">https://en.wikipedia.org/wiki/List_of_Intel_Core_i5_microprocessors</a>) (400, 500 series) Intel Core i3 (<a href="https://en.wikipedia.org/wiki/List_of_Intel_Core_i3_microprocessors">https://en.wikipedia.org/wiki/List_of_Intel_Core_i3_microprocessors</a>) (300 series) Intel Pentium (<a href="https://en.wikipedia.org/wiki/Pentium">https://en.wikipedia.org/wiki/Pentium</a>) (P6000 series) Intel Celeron (<a href="https://en.wikipedia.org/wiki/Celeron">https://en.wikipedia.org/wiki/Celeron</a>) (P4000 series)</p>	<p>Notebook</p>	<p>rPGA (<a href="https://en.wikipedia.org/wiki/Pin_grid_array#rPGA">https://en.wikipedia.org/wiki/Pin_grid_array#rPGA</a>)</p>	<p>988</p>	<p>2.5 GT/s, 4.8 GT/s</p>	
		<p>AMD Phenom II (<a href="https://en.wikipedia.org/wiki/Phenom_II">https://en.wikipedia.org/wiki/Phenom_II</a>) AMD</p>			<p>941[2] (<a href="https://en.wikipedia.org/wiki/CP">https://en.wikipedia.org/wiki/CP</a></p>		<p>S p]</p>

<b>Socket AM3</b> ( <a href="https://en.wikipedia.org/wiki/Socket_AM3">https://en.wikipedia.org/wiki/Socket_AM3</a> )	2009	Athlon II ( <a href="https://en.wikipedia.org/wiki/Athlon_II">https://en.wikipedia.org/wiki/Athlon_II</a> ) AMD Sempron ( <a href="https://en.wikipedia.org/wiki/Sempron">https://en.wikipedia.org/wiki/Sempron</a> ) AMD Opteron ( <a href="https://en.wikipedia.org/wiki/Opteron">https://en.wikipedia.org/wiki/Opteron</a> ) (1300 series)	Desktop	PGA	U_socket#cite_note-941n or 940[3] ( <a href="https://en.wikipedia.org/wiki/CPU_socket#cite_note-940n">https://en.wikipedia.org/wiki/CPU_socket#cite_note-940n</a> )	200–3200 MHz	RAKIP_Açık Sözlük
<b>LGA 1156</b> ( <a href="https://en.wikipedia.org/wiki/LGA_1156">https://en.wikipedia.org/wiki/LGA_1156</a> )/ <b>Socket H</b>	2009	Intel Core i7 ( <a href="https://en.wikipedia.org/wiki/List_of_Intel_Core_i7_microprocessors">https://en.wikipedia.org/wiki/List_of_Intel_Core_i7_microprocessors</a> ) (800 series) Intel Core i5 ( <a href="https://en.wikipedia.org/wiki/List_of_Intel_Core_i5_microprocessors">https://en.wikipedia.org/wiki/List_of_Intel_Core_i5_microprocessors</a> ) (700, 600 series) Intel Core i3 ( <a href="https://en.wikipedia.org/wiki/List_of_Intel_Core_i3_microprocessors">https://en.wikipedia.org/wiki/List_of_Intel_Core_i3_microprocessors</a> ) (500 series) Intel Xeon ( <a href="https://en.wikipedia.org/wiki/Xeon">https://en.wikipedia.org/wiki/Xeon</a> ) (X3400, L3400)	Desktop	LGA ( <a href="https://en.wikipedia.org/wiki/Land_grid_array">https://en.wikipedia.org/wiki/Land_grid_array</a> )	1156	2.5 GT/s	DeMistix

		series) Intel Pentium ( <a href="https://en.wikipedia.org/wiki/Pentium">https://en.wikipedia.org/wiki/Pentium</a> ) (G6000 series) Intel Celeron ( <a href="https://en.wikipedia.org/wiki/Celeron">https://en.wikipedia.org/wiki/Celeron</a> ) (G1000 series)					
<b>Socket G34</b> ( <a href="https://en.wikipedia.org/wiki/Socket_G34">https://en.wikipedia.org/wiki/Socket_G34</a> )	2010	AMD ( <a href="https://en.wikipedia.org/wiki/Advanced_Micro_Devices">https://en.wikipedia.org/wiki/Advanced_Micro_Devices</a> ) Opteron ( <a href="https://en.wikipedia.org/wiki/Opteron">https://en.wikipedia.org/wiki/Opteron</a> ) (6000 series)	Server	LGA	1974	200–3200 MHz	R F a.c
<b>Socket C32</b> ( <a href="https://en.wikipedia.org/wiki/Socket_C32">https://en.wikipedia.org/wiki/Socket_C32</a> )	2010	AMD ( <a href="https://en.wikipedia.org/wiki/Advanced_Micro_Devices">https://en.wikipedia.org/wiki/Advanced_Micro_Devices</a> ) Opteron ( <a href="https://en.wikipedia.org/wiki/Opteron">https://en.wikipedia.org/wiki/Opteron</a> ) (4000 series)	Server	LGA	1207	200–3200 MHz	R F a.c S s: ki
<b>LGA 1248</b> ( <a href="https://en.wikipedia.org/wiki/LGA_1248">https://en.wikipedia.org/wiki/LGA_1248</a> )	2010	Intel Intel Itanium 9300-series ( <a href="https://en.wikipedia.org/wiki/Itanium#Itanium">https://en.wikipedia.org/wiki/Itanium#Itanium</a> )	Server	LGA ( <a href="https://en.wikipedia.org/wiki/Land_grid_array">https://en.wikipedia.org/wiki/Land_grid_array</a> )	1248	4.8 GT/s	

48)		<a href="#">_9300_.28Tukwila.29:_2010)</a>					
<b>LGA 1567</b> ( <a href="https://en.wikipedia.org/wiki/LGA_1567">https://en.wikipedia.org/wiki/LGA_1567</a> )	2010	Intel Intel Xeon 6500/7500-series 9 ( <a href="https://en.wikipedia.org/wiki/Xeon#Beckton">https://en.wikipedia.org/wiki/Xeon#Beckton</a> )	Server	LGA ( <a href="https://en.wikipedia.org/wiki/Land_grid_array">https://en.wikipedia.org/wiki/Land_grid_array</a> )	1567	4.8–6.4 GT/s	
<b>LGA 1155</b> ( <a href="https://en.wikipedia.org/wiki/LGA_1155">https://en.wikipedia.org/wiki/LGA_1155</a> )/ <b>Socket H2</b>	2011/Q1 2011.01.09	Intel Sandy Bridge 9 ( <a href="https://en.wikipedia.org/wiki/Sandy_Bridge">https://en.wikipedia.org/wiki/Sandy_Bridge</a> ) Intel Ivy Bridge ( <a href="https://en.wikipedia.org/wiki/Ivy_Bridge_(microarchitecture)">https://en.wikipedia.org/wiki/Ivy_Bridge_(microarchitecture)</a> ) Intel Xeon E3 12xx Sandy Bridge 12xx Ivy Bridge 12xxV2	Desktop Server	LGA ( <a href="https://en.wikipedia.org/wiki/Land_grid_array">https://en.wikipedia.org/wiki/Land_grid_array</a> )	1155	5.7 GT/s	S su P pe re: Iv su P pe re: Ir S
<b>LGA 2011</b> ( <a href="https://en.wikipedia.org/wiki/LGA_2011">https://en.wikipedia.org/wiki/LGA_2011</a> )		Intel Core i7 3xxx Sandy Bridge-E ( <a href="https://en.wikipedia.org/wiki/Sandy_Bridge-E">https://en.wikipedia.org/wiki/Sandy_Bridge-E</a> ) Intel Core i7 4xxx Ivy Bridge-E ( <a href="https://en.wikipedia.org/wiki/Ivy_Bridge-E">https://en.wikipedia.org/wiki/Ivy_Bridge-E</a> )		LGA ( <a href="https://en.wikipedia.org/wiki/LGA_2011">https://en.wikipedia.org/wiki/LGA_2011</a> )			S E B b P pe



<a href="#">iki/LGA_2011)/</a> <b>Socket R</b>	2011/Q3 (2011.11.14)	Intel Xeon E5 2xxx/4xxx (Sandy Bridge EP) (2/4S) Intel Xeon E5-2xxx/4xxx v2 (Ivy Bridge EP) (2/4S)	Desktop Server	<a href="#">pedia.org/wiki/Land_grid_array)</a>	2011	4.8–6.4 GT/s	<a href="#">re: Ufcsc4C</a>
<b>rPGA 988B</b> ( <a href="https://en.wikipedia.org/wiki/Socket_G2">https://en.wikipedia.org/wiki/Socket_G2</a> )/ <b>Socket G2</b>	2011	Intel Core i7 ( <a href="https://en.wikipedia.org/wiki/List_of_Intel_Core_i7_microprocessors">https://en.wikipedia.org/wiki/List_of_Intel_Core_i7_microprocessors</a> ) (2000, 3000 series) Intel Core i5 ( <a href="https://en.wikipedia.org/wiki/List_of_Intel_Core_i5_microprocessors">https://en.wikipedia.org/wiki/List_of_Intel_Core_i5_microprocessors</a> ) (2000, 3000 series) Intel Core i3 ( <a href="https://en.wikipedia.org/wiki/List_of_Intel_Core_i3_microprocessors">https://en.wikipedia.org/wiki/List_of_Intel_Core_i3_microprocessors</a> ) (2000, 3000 series)	Notebook	<b>rPGA</b> ( <a href="https://en.wikipedia.org/wiki/Pin_grid_array#rPGA">https://en.wikipedia.org/wiki/Pin_grid_array#rPGA</a> )	988	2.5 GT/s, 4.8 GT/s	
		AMD					

<b>Socket FM1</b> ( <a href="https://en.wikipedia.org/wiki/Socket_FM1">https://en.wikipedia.org/wiki/Socket_FM1</a> )	2011	Llano Processors ( <a href="https://en.wikipedia.org/wiki/AMD_Accelerated_Processing_Unit">https://en.wikipedia.org/wiki/AMD_Accelerated_Processing_Unit</a> )	Desktop	PGA	905		U g
<b>Socket FS1</b> ( <a href="https://en.wikipedia.org/wiki/Socket_FS1">https://en.wikipedia.org/wiki/Socket_FS1</a> )	2011	AMD Llano Processors ( <a href="https://en.wikipedia.org/wiki/AMD_Accelerated_Processing_Unit">https://en.wikipedia.org/wiki/AMD_Accelerated_Processing_Unit</a> )	Notebook	PGA	722		U g M
<b>Socket AM3+</b> ( <a href="https://en.wikipedia.org/wiki/Socket_AM3+">https://en.wikipedia.org/wiki/Socket_AM3+</a> )	2011	AMD FX Vishera ( <a href="https://en.wikipedia.org/wiki/Bulldozer_(microarchitecture)#2nd_Generation_Piledriver_core">https://en.wikipedia.org/wiki/Bulldozer_(microarchitecture)#2nd_Generation_Piledriver_core</a> ) AMD FX Zambezi ( <a href="https://en.wikipedia.org/wiki/Bulldozer_(microarchitecture)">https://en.wikipedia.org/wiki/Bulldozer_(microarchitecture)</a> ) AMD Phenom II ( <a href="https://en.wikipedia.org/wiki/AMD_Phenom_II">https://en.wikipedia.org/wiki/AMD_Phenom_II</a> ) AMD Athlon II ( <a href="https://en.wikipedia.org/wiki/Athlon_II">https://en.wikipedia.org/wiki/Athlon_II</a> ) AMD Sempron ( <a href="https://en.wikipedia.org/wiki/Sempron">https://en.wikipedia.org/wiki/Sempron</a> )	Desktop	PGA	942 (CPU 71pin)		

		<a href="https://en.wikipedia.org/wiki/Seampron">https://en.wikipedia.org/wiki/Seampron</a> )					
<b>Socket FM2</b> ( <a href="https://en.wikipedia.org/wiki/Socket_FM2">https://en.wikipedia.org/wiki/Socket_FM2</a> )	2012	AMD Trinity Processors ( <a href="https://en.wikipedia.org/wiki/AMD_Accelerated_Processing_Unit#Trinity">https://en.wikipedia.org/wiki/AMD_Accelerated_Processing_Unit#Trinity</a> )	Desktop	PGA	904		Ug
<b>LGA 1150</b> ( <a href="https://en.wikipedia.org/wiki/LGA_1150">https://en.wikipedia.org/wiki/LGA_1150</a> )/ <b>Socket H3</b>	2013.06.03 2014.05.11 (2015.06.02)	Intel Haswell ( <a href="https://en.wikipedia.org/wiki/Haswell_(microarchitecture)">https://en.wikipedia.org/wiki/Haswell_(microarchitecture)</a> ) Intel Haswell Refresh ( <a href="https://en.wikipedia.org/wiki/Haswell_(microarchitecture)#REFRESH">https://en.wikipedia.org/wiki/Haswell_(microarchitecture)#REFRESH</a> ) Intel Broadwell ( <a href="https://en.wikipedia.org/wiki/Broadwell_(microarchitecture)">https://en.wikipedia.org/wiki/Broadwell_(microarchitecture)</a> )	Desktop	LGA ( <a href="https://en.wikipedia.org/wiki/Land_grid_array">https://en.wikipedia.org/wiki/Land_grid_array</a> )	1150		u: 41 (F R p)
<b>Socket G3</b> ( <a href="https://en.wikipedia.org/wiki/Intel_Socket_G3">https://en.wikipedia.org/wiki/Intel_Socket_G3</a> )	2013/Q2	Intel Haswell ( <a href="https://en.wikipedia.org/wiki/Haswell_(microarchitecture)">https://en.wikipedia.org/wiki/Haswell_(microarchitecture)</a> ) Intel Broadwell ( <a href="https://en.wikipedia.org/wiki/Broadwell_(microarchitecture)">https://en.wikipedia.org/wiki/Broadwell_(microarchitecture)</a> )	Notebook	rPGA ( <a href="https://en.wikipedia.org/wiki/Pin_grid_array#rPGA">https://en.wikipedia.org/wiki/Pin_grid_array#rPGA</a> )	946		

		<a href="https://en.wikipedia.org/wiki/Broadwell_(microarchitecture)">pedia.org/wiki/Broadwell_(microarchitecture))</a>					
<b>Socket FM2+</b> ( <a href="https://en.wikipedia.org/wiki/Socket_FM2+">https://en.wikipedia.org/wiki/Socket_FM2+</a> )	2014	AMD Kaveri ( <a href="https://en.wikipedia.org/wiki/AMD_Accelerated_Processing_Unit">https://en.wikipedia.org/wiki/AMD_Accelerated_Processing_Unit</a> ) and Godavari Processors ( <a href="https://en.wikipedia.org/wiki/AMD_Accelerated_Processing_Unit">https://en.wikipedia.org/wiki/AMD_Accelerated_Processing_Unit</a> )	Desktop	PGA ( <a href="https://en.wikipedia.org/wiki/Pin_grid_array">https://en.wikipedia.org/wiki/Pin_grid_array</a> )	906	?	CAP (h g/ ed (t "I " .w D_ sin
<b>Socket AM1</b> ( <a href="https://en.wikipedia.org/wiki/Socket_AM1">https://en.wikipedia.org/wiki/Socket_AM1</a> )	2014	AMD Athlon ( <a href="https://en.wikipedia.org/wiki/Athlon">https://en.wikipedia.org/wiki/Athlon</a> ) AMD Sempron ( <a href="https://en.wikipedia.org/wiki/Sempron">https://en.wikipedia.org/wiki/Sempron</a> )	Desktop	PGA ( <a href="https://en.wikipedia.org/wiki/Pin_grid_array">https://en.wikipedia.org/wiki/Pin_grid_array</a> )	721	?	CAC (t "I .w D_ sin
<b>LGA 1151</b> ( <a href="https://en.wikipedia.org/wiki/LGA_1151">https://en.wikipedia.org/wiki/LGA_1151</a> )	2015	Intel Skylake ( <a href="https://en.wikipedia.org/wiki/Skylake_(microarchitecture)">https://en.wikipedia.org/wiki/Skylake_(microarchitecture)</a> ) Intel Kaby Lake ( <a href="https://en.wikipedia.org/wiki/Kaby_Lake">https://en.wikipedia.org/wiki/Kaby_Lake</a> )	Desktop Server	LGA ( <a href="https://en.wikipedia.org/wiki/Land_grid_array">https://en.wikipedia.org/wiki/Land_grid_array</a> )	1151		u: 61 (S 71 (F p1

<b>LGA 3647</b> ( <a href="https://en.wikipedia.org/wiki/LGA_3647">https://en.wikipedia.org/wiki/LGA_3647</a> )	2016	Intel Xeon Phi ( <a href="https://en.wikipedia.org/wiki/Xeon_Phi">https://en.wikipedia.org/wiki/Xeon_Phi</a> )	Server	LGA ( <a href="https://en.wikipedia.org/wiki/Land_grid_array">https://en.wikipedia.org/wiki/Land_grid_array</a> )	3647	?	us X p1
<b>Socket AM4</b> ( <a href="https://en.wikipedia.org/wiki/Socket_AM4">https://en.wikipedia.org/wiki/Socket_AM4</a> )	2017	AMD Ryzen	Desktop	PGA	1331	?	co al p1 o1 al
<b>Socket name</b>	<b>Year of introduction</b>	<b>CPU families supported</b>	<b>Computer type</b>	<b>Package</b>	<b>Pin count</b>	<b>Bus clock and transfers</b>	<b>N</b>



# Answer Key





# Chapter 1: Hardware 1.1 (901.1)

1. 184
2. 240
3. 184
4. Error Correcting Code
5. 72  
144  
200  
204
6. PC1600
7. 250
8. PC3-12800
9. Yes
10. RDRAM to terminate
11. Dual Inline Memory Module



# Chapter 4: Networking (901.2)

## 901.2.1 Identify the various types of network cables and connectors

1.
  - 1
  - 2
  - 3
  - 6
2. Multimode fiber
3. T568A
4. Satellite TV  
Cable TV
5. 2

## 901.2.2 Compare and contrast the characteristics of connectors and cabling

1. Time Domain Reflectometer
2. Star
3. Bus
4. Microwave ovens  
Cordless phones
5. Plenum

## 901.2.3 Explain the properties and characteristics of TCP/IP

1. To send data outside of your area of the network
2. 510
3. D
4. To check that the network card is able to transmit and receive
5. The DHCP server cannot be reached

## 901.2.4 Explain common TCP and UDP ports, protocols, and their purpose

1. 25 and 110
2. TCP
3. 22 and 3389
4. SNMP
5. It is designed to group DNS objects together (for example, Address records for

that domain)

### **901.2.5 Compare and contrast various Wi-Fi networking standards and encryption types**

1. Temporal Key (TKIP)
2. WEP
3. 600Mb/s
4. 802.11n and 802.11ac
5. WPA2

### **901.2.6 Given a scenario, install and configure SOHO wireless/wired router and apply appropriate settings**

1. Quality of Service (QoS)
2. The scope defines a range of IP addresses that can be leased to other network components and end devices.
3. 8 days, 1 hour.
4. File server for public use  
SharePoint access for external users  
Federation and single-sign on for staff connecting externally  
Honeypot to trap possible attackers  
Web server to host a public-facing website with no confidential or sensitive information.
5. This is the edge firewall exposed to the internet. All traffic leaving the domain is checked at this point. All incoming traffic is checked as to its purpose and only legitimate traffic entering on open ports is allowed access.

### **901.2.7 Compare and contrast internet connection types, network types and their features**

1. MAN
2. PAN
3. LAN
4. Current 4G transfer rates are 300 Mb/s
5. Laying additional fiber to every household from the cabinet is costly, when coaxial will meet bandwidth demand

### **901.2.8 Compare and contrast network architecture devices, their functions, and**

## **their features**

1. Router
2. Switch (This is VLAN)
3. Bridge
4. Firewall
5. Hub

## **901.2.9 Given a scenario, use appropriate networking tools**

1. Crimper
2. WiGLE (or alternative smartphone app)
3. 110 block/patch panel/RJ45 wall socket
4. Voltage  
Current  
Resistance
5. A Main or Intermediate Distribution Frame to find the end of a cable.



# Chapter 5: Mobile Devices (901.3)

1. Press and hold the Detach key until the light on the key turns greenPull the screen away from the keyboard. You'll have a few seconds to detach it before it reconnects automatically.
2. Surface Book uses battery power to detach the keyboard. If battery power is low, you'll have to wait until your Surface Book has recharged before detaching it.
3. Expresscard 34  
Expresscard 54  
PCMCIA  
SODIMM

Explanation: The 54 is in fact a 34mm slot with a protruding L-shape section and accepts both the 34 and 54 card.

4. Hybrid  
Solid-State  
Mechanical  
Optical

Explanation: Optical is not a hard drive type. Hybrid and Mechanical both have some mechanical components which may be jarred on impact. Solid-State as the name suggests is a series of chips and as long as no physical damage comes to the chips the data will be intact.

5. Older laptop screens use a fluorescent light to 'backlight' the screen. This is AC powered however the laptop uses DC power provided by the battery. The job of the inverter is to generate AC power from DC power in order to power the fluorescent bulb.
6. Laptops feature multi-purpose keys used for media play and control. These are used to play, rewind/fast-forward, stop and skip tracks. They control the primary media player app installed on the device.
7. Typically if using HDMI a 'wake' signal is sent to the device to notify it that the new video data is being sent on a specific input channel, so the device switches over to the correct input. Assuming that the monitor is on the correct input and the

screen is blank anyway, the OS may not be projecting to the device. On Windows Systems, the Windows key + P is a quick way to get to the Project screen. Alternatively you can use the 'Project to a second screen' system settings page. Here, the options are for PC Screen Only, Duplicate, Extend or for the Second Screen only. In the above scenario Project is set to PC Screen only. If this is changed to Extend or Duplicate then video data will be seen on both monitors.

8. A Barrel/Kensington lock is a physical lock with a steel cable allowing you to connect direct to the frame of the laptop and to attach it to the desk, impeding theft.
9. In public spaces the wearer would be distracted by information presented on the lenses and less aware of their surroundings. This is extremely dangerous when, for example, crossing a busy road. Furthermore, there have been cases where the wearer was cycling, and others of the user driving a car.
10. This is known as tethering. The laptop is connecting to the mobile phone which is acting as a Wi-Fi hotspot. The mobile may be able to connect to the hotel's Wi-Fi router where the laptop cannot (for example, due to compatibility issues), or mobile data on the mobile can be used instead. The connection can be secured so that only the laptop connects to the hotspot. This can be done with a mutual password used on both devices, or by physically connecting the laptop to the mobile phone using a USB cable.





# Chapter 6: Hardware and Network Troubleshooting (901.4)

1. The problem is a physical one, not due to the OS. Given this we need to consider the environment. The rack enclosure is a large cabinet containing usually a lot of hardware. Given this the hardware generates heat and so air conditioning within the sealed unit is needed. The aircon unit blows cold air through the hardware and the returning heated air is passed into the aircon unit where it is cooled. If the cold isles were obstructed, a processor fan within the server is not working, or the aircon unit was not powerful enough to deal with the heat within the enclosure heat will build up over time. Given that the server is working for long enough for the OS to boot and work for some time, the implication is that the heat buildup is gradual. If the CPU fans in the server were not working at all, then it is likely the OS would not have sufficient time to boot up.
2. It is common to find that blade servers are modular with around 8-12 processors within the drawer. The CPU fans are also modular and are easily removable. The problem being described here is common with HP blade systems. If one CPU fan fails, the server increases the speed of the other fans significantly to continue airflow through the blade (hence the noise). If two modules fail the server will be unable to keep sufficient airflow, so a forced shutdown is triggered.
3. The BIOS may be booting into the wrong hard drive. When an OS is installed the Boot Configuration Database is written. If other OS systems are found, then the new OS is added to the boot list and usually also is made default. It is certainly possible that over time a different BCD was written to another disk. If the BIOS boots into this erroneous disk the BCD loaded will be old and not contain the latest information. Either fix the boot order in the BIOS, or rescan the BCD to find missing OS systems.
4. There are two further tests - first, plug a patch cable from the suspected port to the switch. If the switch status LED lights up we have physical connectivity. This is the same on the NIC as well. In the Windows OS, on the Network Adapters screen the NIC should list as connected. A low-tech solution used when no switch is available would be to use a loopback plug. This is an RJ45 plug with 2 wires completing the data circuit. If the NIC status LED lights up, or Windows reports 'Connected' then the socket itself is not damaged.
5. SMART is a built-in checking mechanism for hard drives. It indicates that the drive

is now not working to expected operational parameters. It may be that the drive is becoming worn. Further use of the drive may cause more damage, or data loss. The recommendation is to remove data from the drive to an alternative location as soon as possible and to replace the drive.

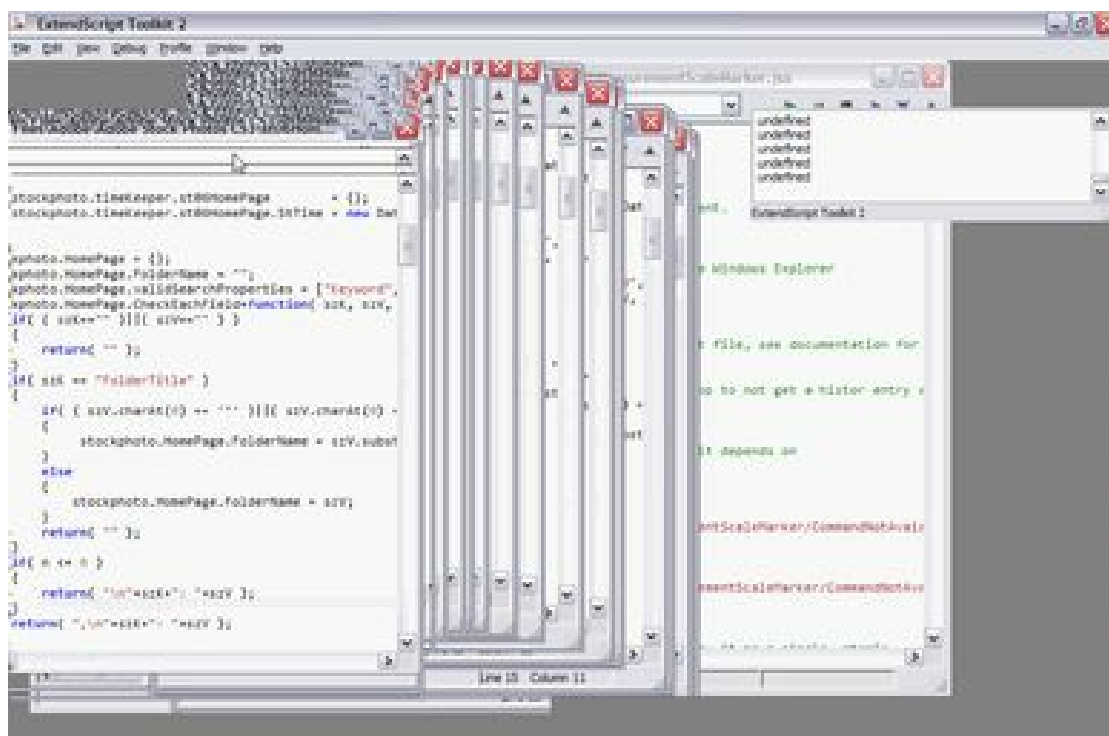
6. The media bay is the front top section of the chassis where the optical drives and floppy drive are fitted. On modern systems the floppy drive section is used to house a front connector panel.

The hard drive enclosure is a steel box below the former floppy drive section. HDDs are screwed to this enclosure which on some chassis is held in place by a latch and is detachable. (section 2 on the photo)



(<http://www.data-r-us.com/images/computer-case-2.jpg>)

7. DISKPART commands can be scripted and added to a deployment.  
Drive letters can be removed, hiding the partition from the OS.  
Active partitions can be made inactive  
For Itanium computers Microsoft Reserved and Extensible Firmware Interface (EFI) partitions can be created.  
A mirrored volume can be broken with the Break Disk command.
8. A series of colour blocks on the monitor. This may suggest a problem with the video card such as overheating, or that the graphics card driver needs to be updated. Some artifacts are caused by the OS not updating the screen properly if a window is moved as in the image following:



9. A monitor is designed to receive images at a set frequency and resolution, known as the native resolution. This is the optimal setting for the device, although it can handle others. Video cards can display a large array of different resolutions and frequencies and if an incompatible frequency is used the monitor cannot 'lock' the signal and so black strobing can be seen. This can be fixed by swapping to an acceptable frequency. In the UK it is common to use 60Hz although gaming systems can use much higher refresh rates.
10. The most obvious fix would be to swap the IP settings to receive a Dynamic address from a DHCP server. With most DHCP scopes you also set scope options and the most obvious to set would be the location of the DNS server. If its IP address has changed everyone else on the network will be aware of the change due to the scope option, but your PC, which is manually configured would not be aware of the change. If you want to keep a manual address you will need to update the IP address of the DNS server. This is done in the NIC's IPv4 / IPv6 properties page. Once completed it is also good practice to flush the local DNS cache to remove any old entries, then perform an NSLOOKUP of a resource to test that you have connectivity to the DNS server.



# Chapter 7: Windows Operating Systems (902.1)

1. Shadow Copies is a tool that tasks the OS to save a new instance of the file to a different part of the volume every time, marking the most recent save as active. A user can choose to recover a previous version, if this is enabled on the volume.
2. ReadyBoost is a feature that enables you to use a USB pen drive as additional RAM.
3. For Windows 8.1 they are Private, Guest, and Public are now combined. Private is used when connected to a Domain. Public is used when connected as a standalone PC, or to a public hotspot such as in a cafe.  
Earlier profiles found on Windows 7 were Home (relaxed security for home users), Public, or Work (now known as Private).
4. Windows System Image Manager allows you to create the `unattend.xml` file.
5. The Advanced Boot options menu allows you to resave the system files back into the Windows folder and its subsystem. Refresh uses existing Registry settings, where Reset completely rewrites everything and regenerates the registry. With Reset you need to reinstall your applications and move your user data onto the newly created user account. These options have been rebranded on each version of Windows, so there is often some confusion.
6. `ROBOCOPY` is capable of retrying until the entire contents of the file are copied over. This is the more reliable method than the `COPY` command.
7. `GPRESET` will produce a text report listing all policies being applied to this computer. If the GPO is being applied it will appear in this report.
8. `REGSVR32` can be used to register DLL files into the Registry.
9. First the disk needs tidying of unwanted and unneeded files using the Disk Cleanup utility, or a third-party tool such as CCleaner. Next optimize the disk by running the built-in Defragmentation tool, or a third-party tool such as Defraggler.
10. When DHCP is used and common for laptop users Windows will provide an Alternate Configuration tab on the NIC's IPv4 properties page. When connected to the Office network you receive your IP settings through DHCP. At home most likely the IP settings will be different, so the alternative numbers are used when the laptop realizes that no DHCP is available.







# Chapter 8: Other Operating Systems and Technologies (902.2)

1. Time Machine is used to create and restore backups.
2. Filenames, document content, and an internet web page search.
3. iCloud.
4. IWCONFIG is used for wireless NICs (IFCONFIG is incorrect on this occasion as this will show wired NICs).
5. Prefixing the `install` command with `sudo` will elevate just for this command only.
6. Yes. VI allows you to make basic changes to a text file, such as an INI file.
7. Data on a public cloud can be accessed by people who are not members of your organization, where as a private cloud can only be accessed by your internal staff.
8. This allows us to use single sign-on when crossing security boundaries. Our federation proxy server is installed into the perimeter network (DMZ) allowing staff working from home or outside of the domain to access the domain. The session runs on the federation proxy server and is streamed to the user via an encrypted tunnel. A separate encrypted tunnel from the federation proxy server to the federation server itself (which is installed inside of the domain) is used to check the account details and then to establish the session and send domain data to the user.
9. Whether network-based or host-based, detection systems record incidents, but do not necessarily stop the incident from occurring. Intrusion prevention systems actively block any unwarranted or unusual activity. They consume extra processing resources as files and ports are being actively monitored.
10. The cloud resource can be upscaled as needed, based on the resource demand. If the resource reaches its limit, and if the user has given permission for this to happen, then the service plan will be upgraded temporarily. When resources slip back down, the service plan will reduce.



# Chapter 9: Security (902.3)

1. Either with the `TASKKILL` command or by selecting the browser pop-up window from the task list in Task Manager and selecting the End Task action. The reason this happened was that the 'X' button was not a real button - the pop-up window is in fact an animated graphic mocked to look like a real Windows form. The outside of the form and any buttons on the form are part of the picture. Clicking anywhere on the pop-up would trigger the virus to execute.
2. Before connecting the PC to the internet, harden the system by installing the latest service pack and patches. Zero-day attacks are those which target vulnerabilities in the system which have since been patched with updates. As you have only just installed the OS from the disk which may be several years old now, these patches have yet to be applied.
3. A man-in-the-middle attack uses ARP poisoning of two adjacent PCs on the subnet. With this attack, the man-in-the-middle can see all packets sent between the two PCs and from this determine key information, such as hardware passwords. This attack happens locally - the attacker has to be on the same subnet as where the attack is taking place.
4. If your PC is running a background service, which you are unaware of, the PC is said to have no control over this service, hence a zombie. Distributed DOS attacks commonly send out code to run on other PCs across a network which collectively target and flood a resource, such as a router, so that it cannot do its normal job, so legitimate data cannot flow into the network from this point.
5. Entry control. Here a roster (a list of allowed people for the given time period) is provided to a security guard who only allows access to named people on the list. Other staff, although valid employees, are barred access.
6. PLP only gives users access to the resources they need to do their job and only to the level they need. Further privilege has to be requested through a change management process, so is documented. PMP gives too high access permissions to users, so users may accidentally, or deliberately change the security permissions for others, bar users from a folder, or take ownership of files for themselves.
7. User Account Control will stop a standard user from making such a change, instead prompting for an administrator to present their login credentials.
8. Full-disk or volume encryption. Volume encryption is faster but not as secure.
9. You have hidden the SSID. Only known devices have been allowed to connect to

the access point.

10. A certificate of destruction.



# Chapter 10: Software Troubleshooting

## (902.4)

1. From an internet browser, sign into your Google account and go to the Find your phone page. Select the device you want to search for - it will report as close as it can where the device is. If the device is turned off you will see the timestamp for the last time the system sent a handshake to Google. You have the option to send a factory reset.  
Alternatively, contact your mobile provider who is also able to do this for you. Again, you can send a remote wipe to the phone. Once it is switched on it will receive the signal and wipe the contents of the phone.
2. Pokemon Go uses GPS, Location settings, Mobile Data, or Wi-Fi, and also the camera. The Lightsaber app switches on the torch when in use. Both of these will cause a heavy drain on the battery.
3. Encryption is achieved using a certificate file that has to be installed both on the mail server and on the mobile phone. As this is not installed on the phone they will not be able to decrypt the mail messages.
4. I've paired the wrong Bluetooth speakers to my phone, or the other person tried to pair theirs to their phone and selected my phone by mistake.
5. Hold down Power, Volume, and Home for a few seconds.
6. Hold down Power and the Home button for 10 seconds.
7. Not necessarily. Spam is a general email sent to all live accounts. The mail server is correctly identifying it as Spam and redirecting it to the Junk folder. You should educate her to be able to identify spam and show her how, by marking emails in her inbox as spam the system will be trained to automatically categorize more spam than it is at the moment. Also you will want to warn her not to click on any links and the reason for this is that you would be confirming that you are a live user to the spam sender.
8. This is a Spear-Fishing attack. Specific personal information is being used, so the sender clearly did their homework. This may be considered Whaling given the status of the person targeted, but no financial information appeared to have been asked for, or changed hands.
9. The Linux GRUB / LILO boot manager and Windows' BCD are not compatible. When you made manual changes to the partitions Windows found the Linux system, but the GRUB partition may have been deleted. You will need to access GRUB

from the Linux installer disc and repair the GRUB, but if you want the default Boot Manager to be the BCD will have to then go into the Windows Recovery Environment to make the BCD the active partition and may have to point the Linux record to the new location of the GRUB boot partition.

10. BitLocker uses UEFI to ensure that the new BIOS is encrypted. UEFI requires a 64-bit system. The certificate is kept on the TPM chip on the motherboard (although there are other options).





# Chapter 11: Operational Procedures

## (902.5)

1. Turn the power off. Wear anti-static protection. Use a lit area such as a workbench. Put components into anti-static bags. Use the right tools. Be careful of sharp metal. Do not force components to fit.
2. Jewellery is metallic and conductive. You may short a circuit, causing damage as well as giving you a shock.
3. The equipment has moving parts and you might trigger it to cycle the rollers, which could pinch the tie, strangling you, or getting yourself caught in the machinery. No exposed and dangling clothing such as ties should be used where there are moving parts.
4. Disposal instructions, the manufacturer's contact details including where to go for support, ingredients, and health information such as toxicity.
5. This is Digital Rights Management. After 30 days the Kindle account will disable access to the book.
6. This is an example of Personally Identifiable Information.
7. You have no guarantee as to the amount of technical knowledge an end-user has.
8. This is a discussion technique where the listener paraphrases what was said by the speaker so that both parties agree on what was actually said.
9. This has more to do with Customer Service than pride, or technical competence. Agree on what you can of the situation. Agree on an outcome and timescale. Agree to do the parts of the work that are agreed upon. By doing this you can still move forward with the work and will be able to resolve some, if not all of the problem presented to you. Offer options on the parts you cannot resolve.
10. I wanted to say 'get paid' here, but that's not part of the CompTIA troubleshooting theory! You should document your findings and record your actions so that if you or your team encounter the problem again you will be able to know how to resolve it quickly by repeating the solution.